



## ***SecureCom and CMDS Enterprise***

**Stopping  
Insider Abuse and Spying**

**Detecting the hard stuff:  
Stolen passwords, unauthorized records browsing,  
employee espionage, infiltration, and  
insertion of unwelcome code**

**via automatic behavior profiling**

**Dave Steinman, Mike Celiceo, Joe Head  
ODS Networks**

## Form SF298 Citation Data

<b>Report Date</b> <i>("DD MON YYYY")</i> 03061999	<b>Report Type</b> N/A	<b>Dates Covered (from... to)</b> <i>("DD MON YYYY")</i>
<b>Title and Subtitle</b> SecureCom and CMDS Enterprise		<b>Contract or Grant Number</b>
		<b>Program Element Number</b>
<b>Authors</b>		<b>Project Number</b>
		<b>Task Number</b>
		<b>Work Unit Number</b>
<b>Performing Organization Name(s) and Address(es)</b> IATAC Information Assurance Technology Analysis Center 3190 Fairview Park Drive Falls Church VA 22042		<b>Performing Organization Number(s)</b>
<b>Sponsoring/Monitoring Agency Name(s) and Address(es)</b>		<b>Monitoring Agency Acronym</b>
		<b>Monitoring Agency Report Number(s)</b>
<b>Distribution/Availability Statement</b> Approved for public release, distribution unlimited		
<b>Supplementary Notes</b>		
<b>Abstract</b>		
<b>Subject Terms</b>		
<b>Document Classification</b> unclassified		<b>Classification of SF298</b> unclassified
<b>Classification of Abstract</b> unclassified		<b>Limitation of Abstract</b> unlimited
<b>Number of Pages</b> 84		



<b>REPORT DOCUMENTATION PAGE</b>			Form Approved OMB No. 074-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.				
<b>1. AGENCY USE ONLY (Leave blank)</b>		<b>2. REPORT DATE</b> 6/3/99	<b>3. REPORT TYPE AND DATES COVERED</b> Briefing	
<b>4. TITLE AND SUBTITLE</b> SecureCom and CMDS Enterprise			<b>5. FUNDING NUMBERS</b>	
<b>6. AUTHOR(S)</b> Dave Steinman, Mike Celiceo, Joe Head				
<b>7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)</b> IATAC Information Assurance Technology Analysis Center 3190 Fairview Park Drive Falls Church VA 22042			<b>8. PERFORMING ORGANIZATION REPORT NUMBER</b>	
<b>9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)</b> Defense Technical Information Center DTIC-IA 8725 John J. Kingman Rd, Suite 944 Ft. Belvoir, VA 22060			<b>10. SPONSORING / MONITORING AGENCY REPORT NUMBER</b>	
<b>11. SUPPLEMENTARY NOTES</b>				
<b>12a. DISTRIBUTION / AVAILABILITY STATEMENT</b>			<b>12b. DISTRIBUTION CODE</b>  A	
<b>13. ABSTRACT (Maximum 200 Words)</b> This briefing addresses the issue of stopping the insider abuse and spying , which is detecting the hard stuff: Stolen passwords, unauthorized records browsing, employee espionage, infiltration, and insertion of unwelcome code via automatic behavior profiling				
<b>14. SUBJECT TERMS</b> COMP, IA, Biometrics			<b>15. NUMBER OF PAGES</b>	
			<b>16. PRICE CODE</b>	
<b>17. SECURITY CLASSIFICATION OF REPORT</b> Unclassified	<b>18. SECURITY CLASSIFICATION OF THIS PAGE</b> UNCLASSIFIED	<b>19. SECURITY CLASSIFICATION OF ABSTRACT</b> UNCLASSIFIED	<b>20. LIMITATION OF ABSTRACT</b>  None	





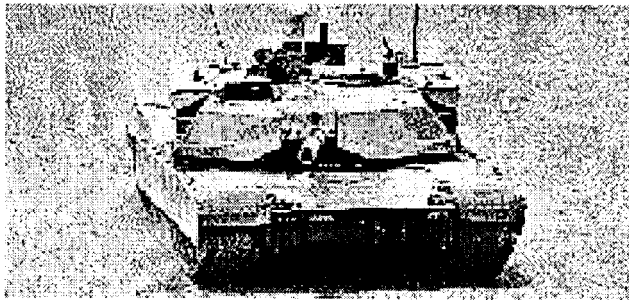
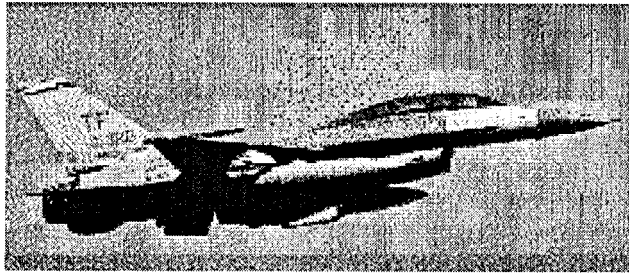
## ***Agenda: Foiling the Bad Guys***

- A quick look at the problem
- An integrated, deployable solution for:
  - Monitoring the network infrastructure
  - Monitoring hosts
  - Conversation monitoring and tracking
  - The truly hardened perimeter
  - The crypto element
  - User behavior analysis
  - THE BIG PROBLEM - event correlation and management
    - New tools applied to an old problem
- What comes next. Scaling to Gigabit speeds.



*Our Subject- Protection of:*

## ***Mission Critical Target Networks***

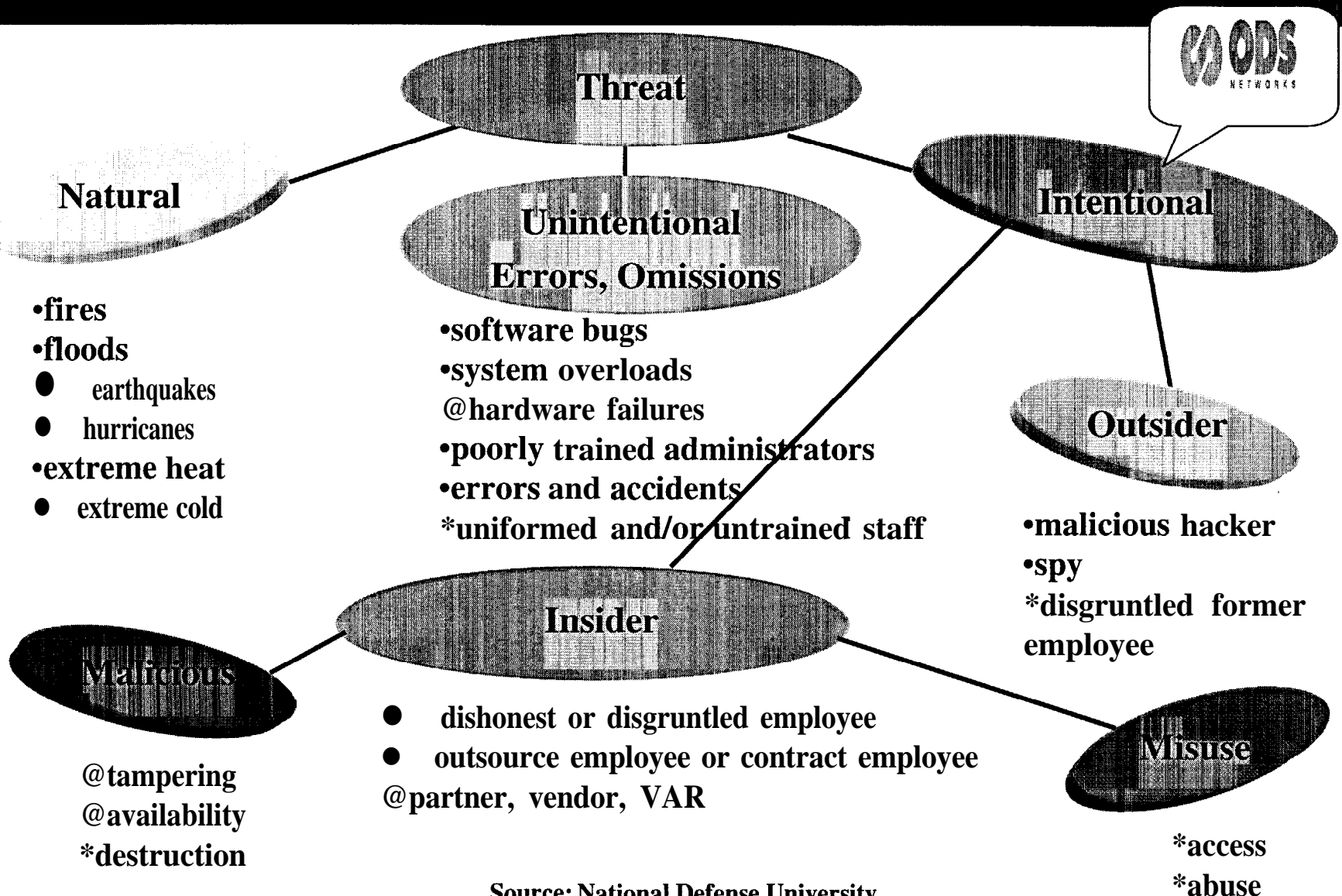




## *Winning War Strategy*

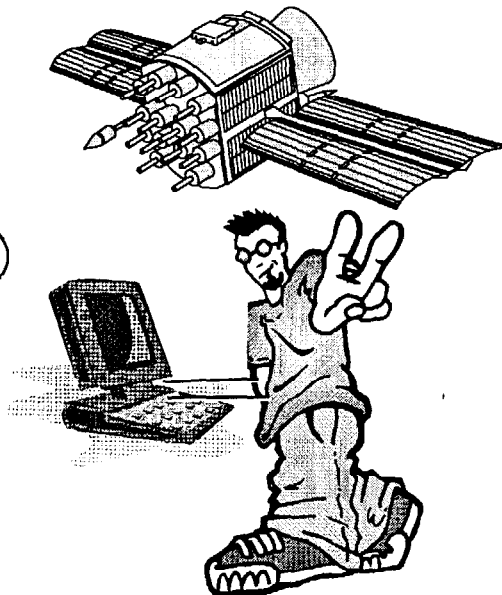
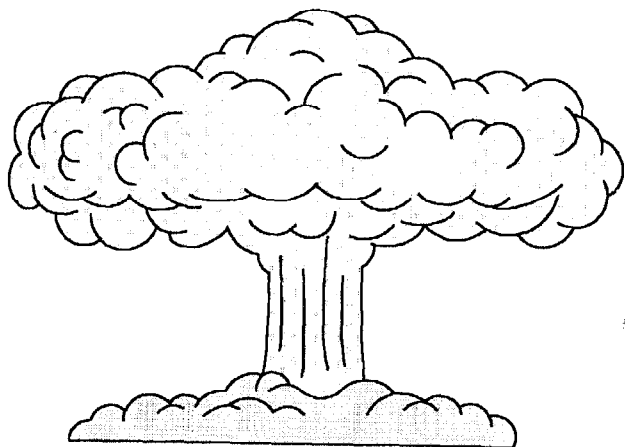
- Put up attacks that the enemy can't defend
- Put up offensive weapons systems for which the enemy can't afford the defensive system
- Strive for large asymmetry: 1 cent attack, \$100 defense

# Threats to Your Network



Source: National Defense University

- **Failing to define the enemy**
  - **Electronic Pearl Harbor Scenario vs espionage**
  - **military adversaries vs hackers with shared tools**
  - **Presence of all 4 creates need for multi-phased defense**

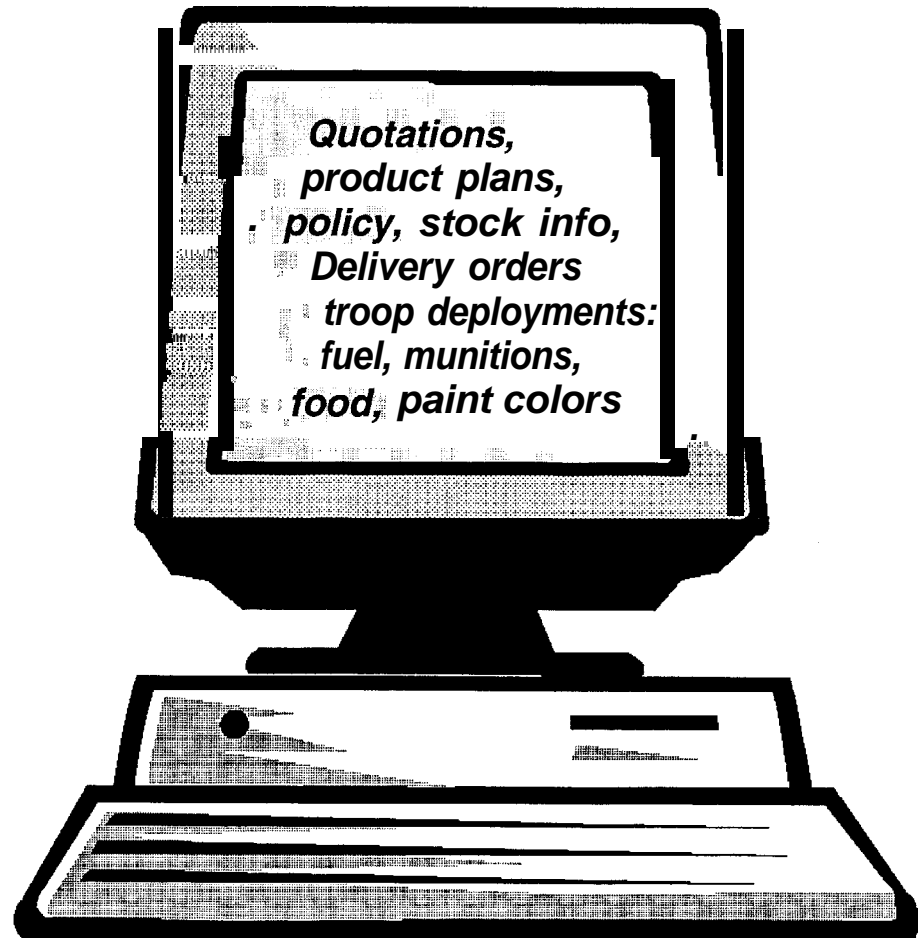


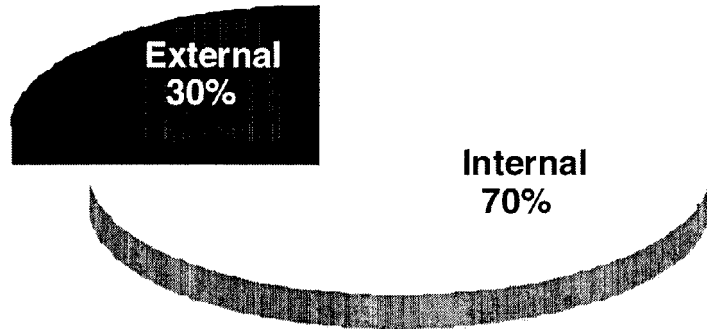
- Who won't
  - Those most likely to be able to
  - Professional corporate spies
  - Intelligence organizations
  - Hackers, spies, and thieves don't harm the Internet, it nukes their sandbox
- Who might:
  - A terrorist group
  - Fringe psychopaths
  - Journeyman invaders
  - Tactical theater enemies

<i>Internal</i>	<i>Yes</i>
<i>External</i>	<i>Yes</i>

## *Covert Cyber Intelligence against the US Infrastructure*

- Attacks against sensitive but unclassified systems is:
  - relatively easy
  - effective
  - non-traceable
  - deadly
  - cheap labor pool ready for work
  - bad asymmetry in both \$ and expert people

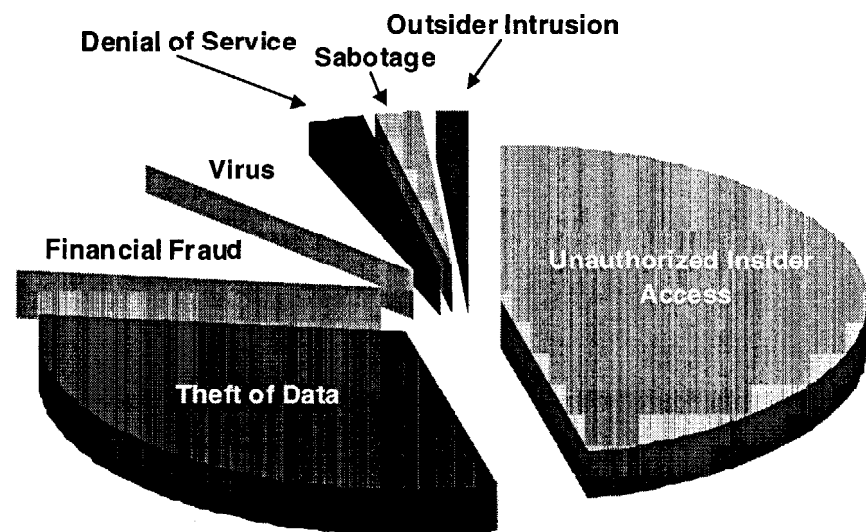




- Percentage 1997 dollar losses for computer and network security events by cause:

- 46% insider misuse
- 32% data theft
- 11% financial fraud
- 7% virus attacks
- 2% sabotage
- 2% outsider penetration

- 70% of security events are by insiders
- Our networks have a hard, crunchy exterior with a soft, squishy interior
- Most security expenditures attempt to solve the wrong problem







## *The smartest penetrators*

- Military or Intelligence staff
- Mercenary hackers who are Warsaw ex-intel
- Target troop, movement, plans, and logistics data
- Steal advanced research and planning data
- Never use shared tools
- Heavy use of spoofing, twin sessions, stolen sessions
- More likely to evade Firewalls and IDS systems

- **Motivations and methods**
  - **Amateur hackers versus strong, well funded adversaries**
  - **Attacks versus industrial espionage**
  - **Mischief versus strategic data collection**
  - **Commonly available hacker tools versus proprietary tools**
  - **The bad guys we easily detect versus the bad guys we never see**
- **We need to protect against all threats, inside and outside.**



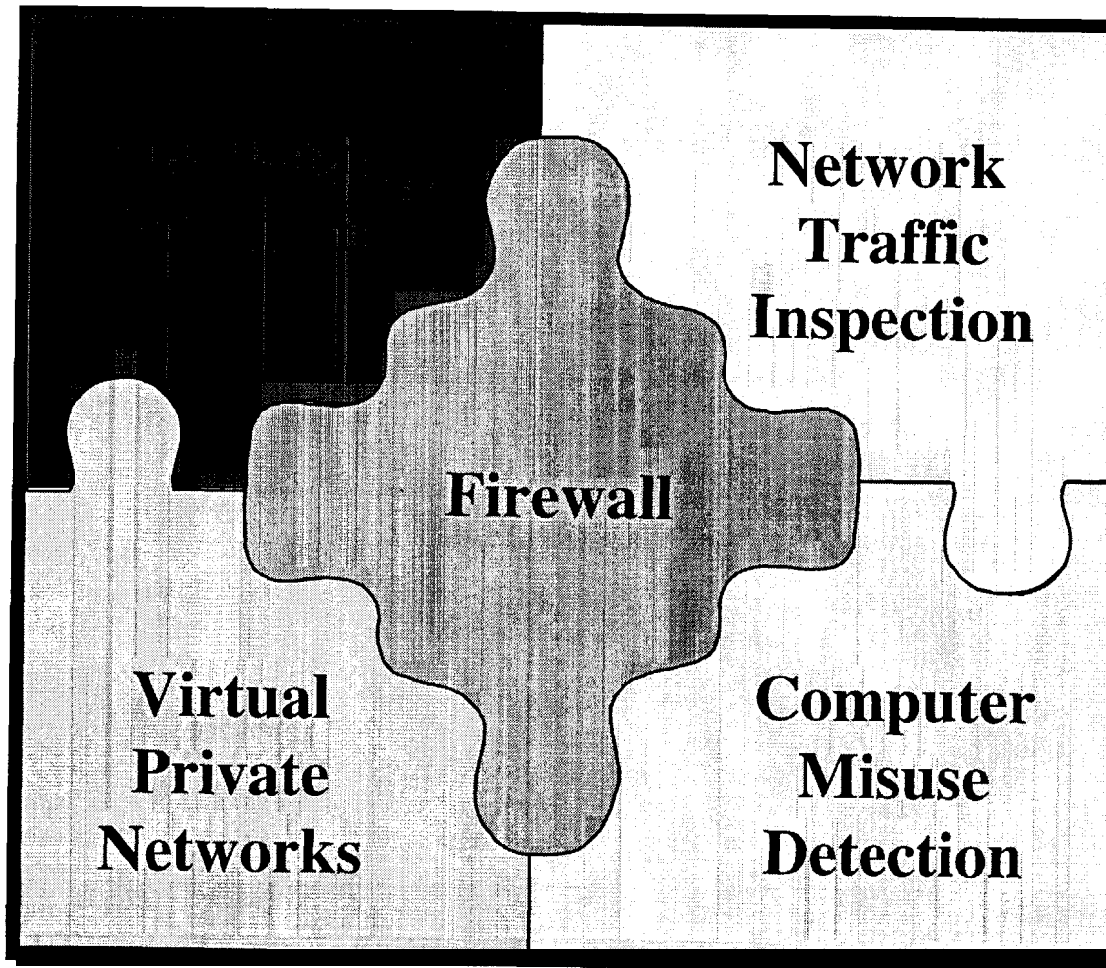
# ***An Integrated Infrastructure Defense***

***A Modular, Scalable, Layered,  
Coordinated Multi-vendor Defense***

***Joe Head  
head@ods.com  
972/301-3636***

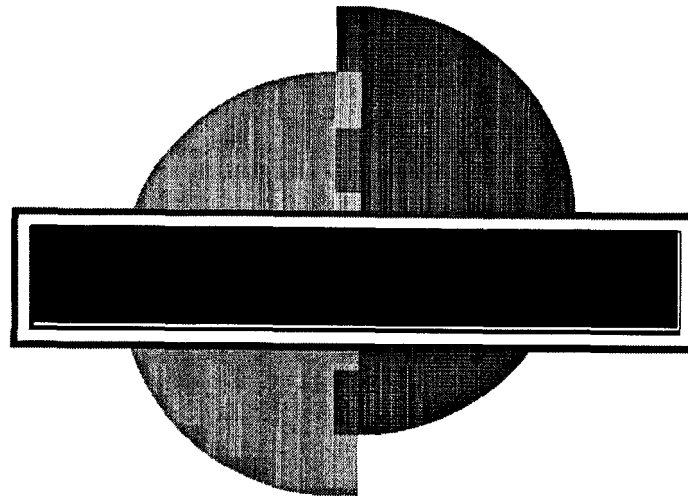


## *Enterprise Network Security*





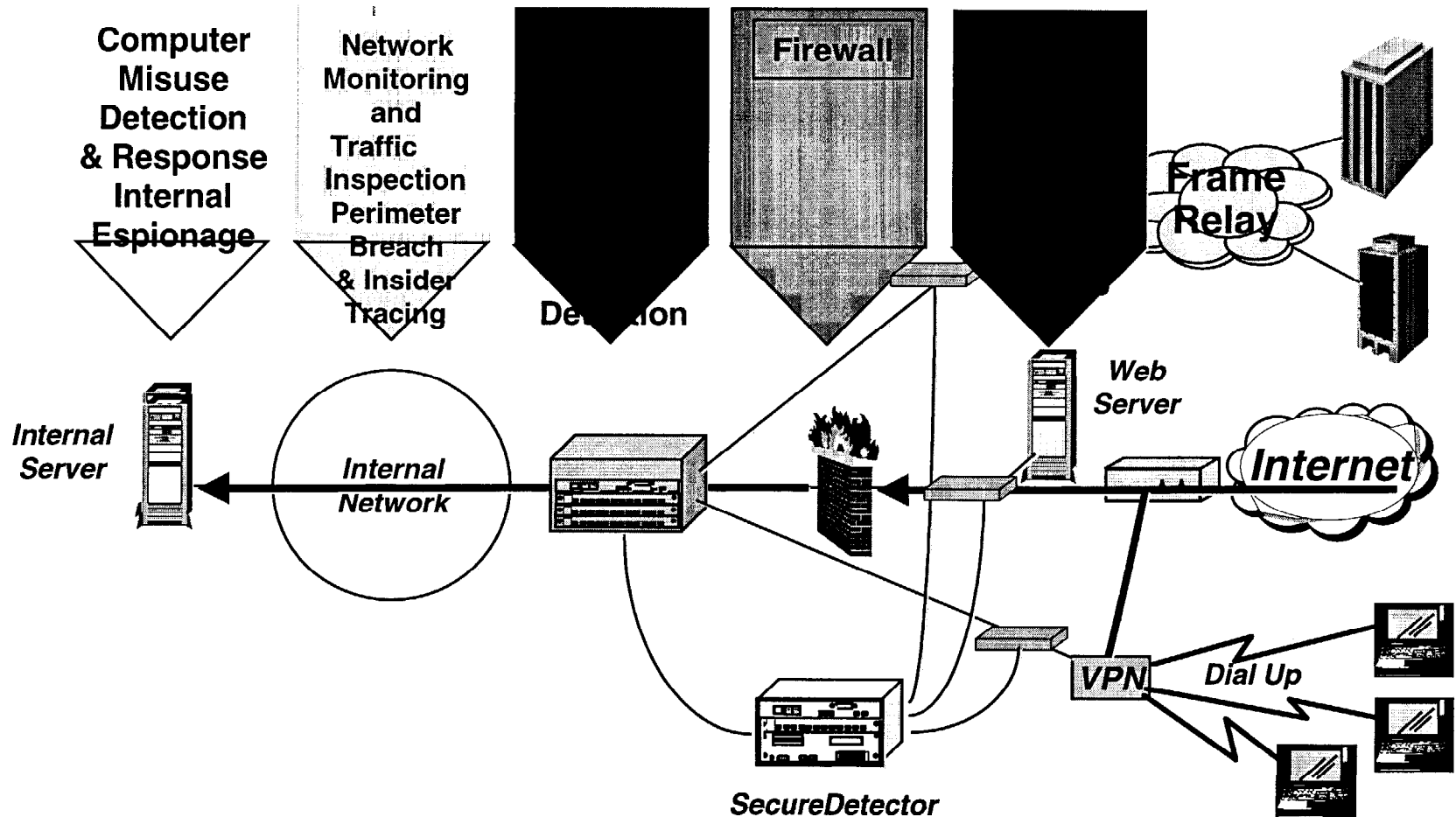
*Extreme Access . . .  
Infinite Possibilities*



*A Field Deployable,  
Modular, Scalable  
Multivendor Security Solution*

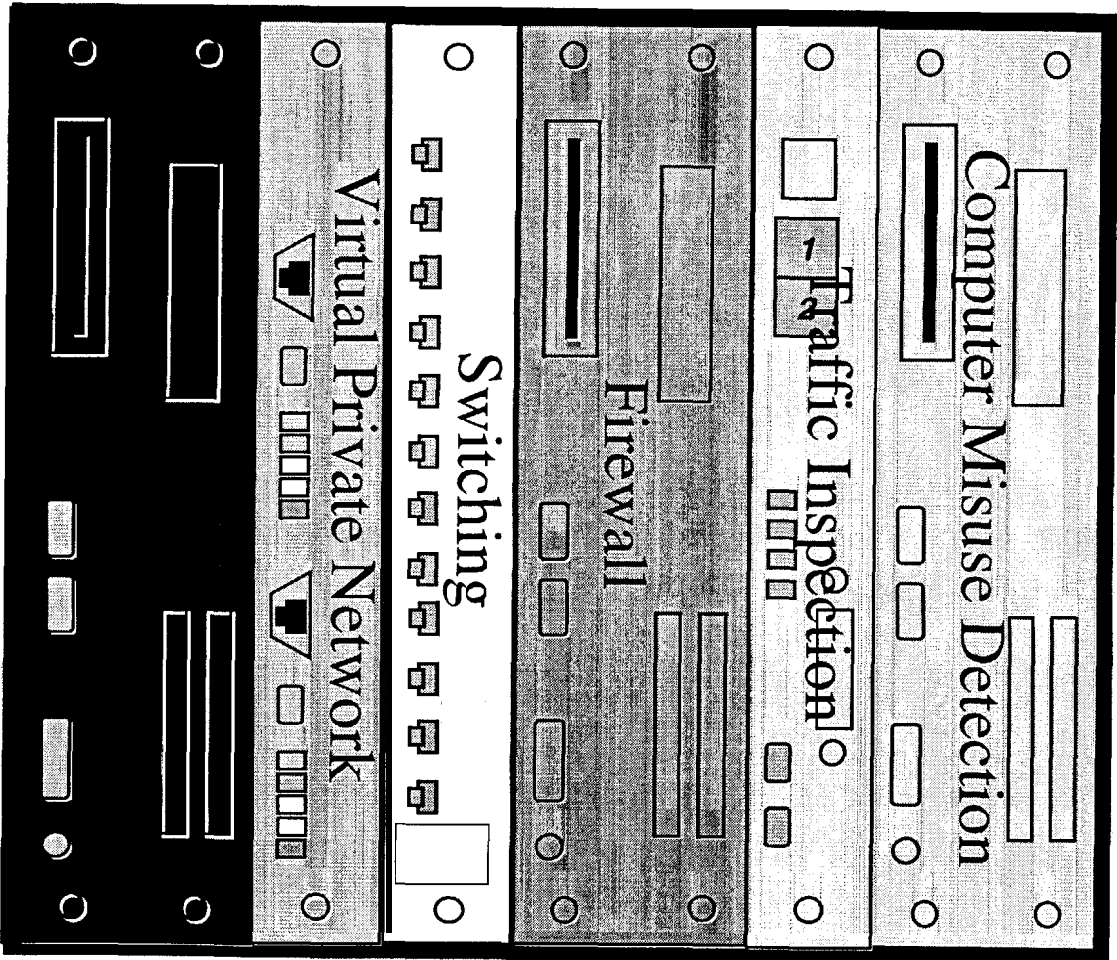


# SecureCom Integrates Protection At All Critical Places



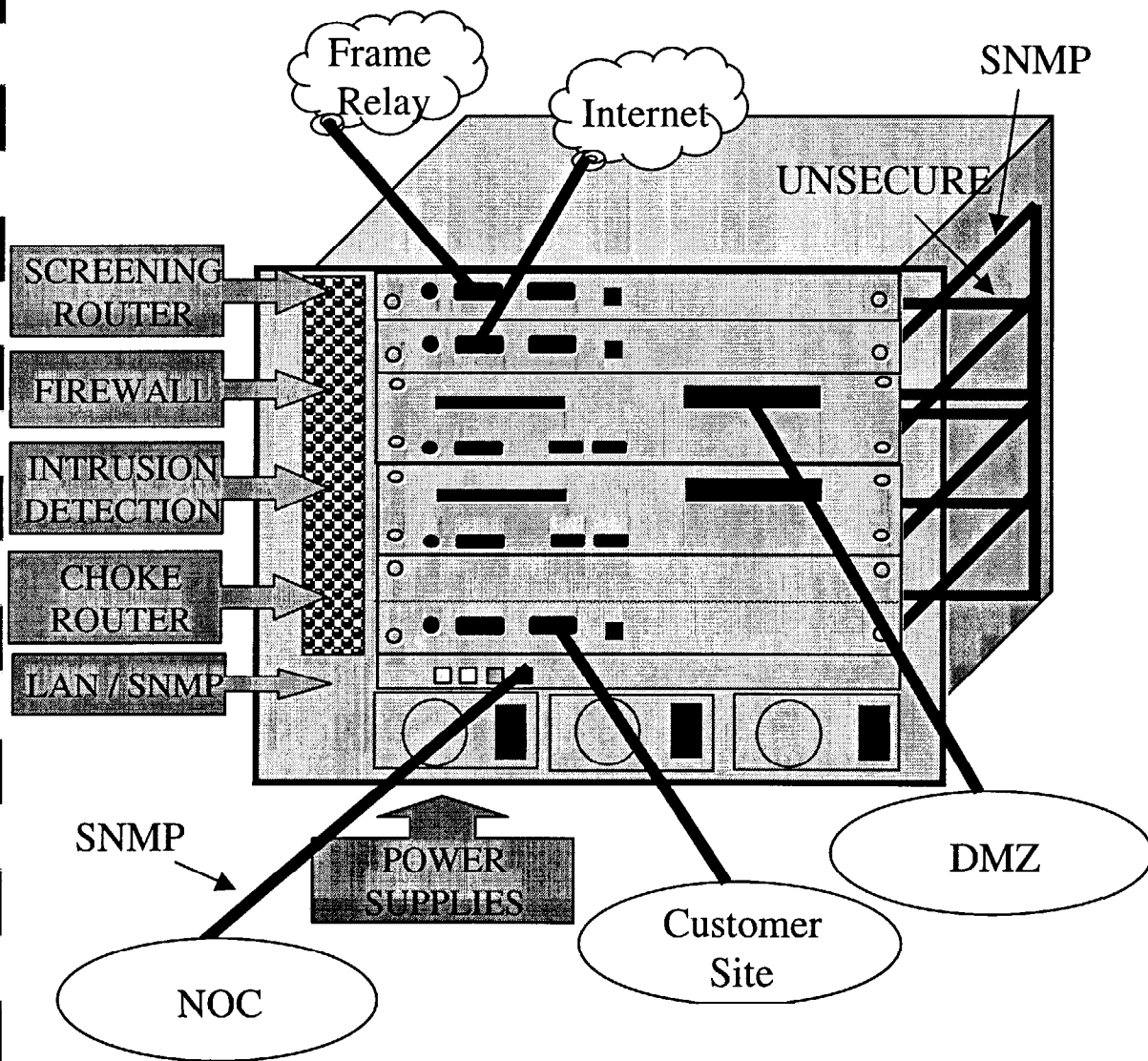


# ODS Networks SecureCom Platform





# SecureCom; Internet Security Device



## Specifications:

Use	Easy to Install Easy to Configure Easy to Support Easy to Troubleshoot
LAN	Ethernet
Chassis	Base Unit N + 1 Power Designed for NEBS
Modules	How Swappable
BUS	100mbps Switched Shared Management
Manage	SNMP & RMON Out of band, encrypted
Router	Any Cisco, COTS, SW
Firewall	FW1, LMF, Raptor, etc.
Processor	Intel Sparc
O/S	NT X.86 Unix
Audit	Remote Log to CMDS





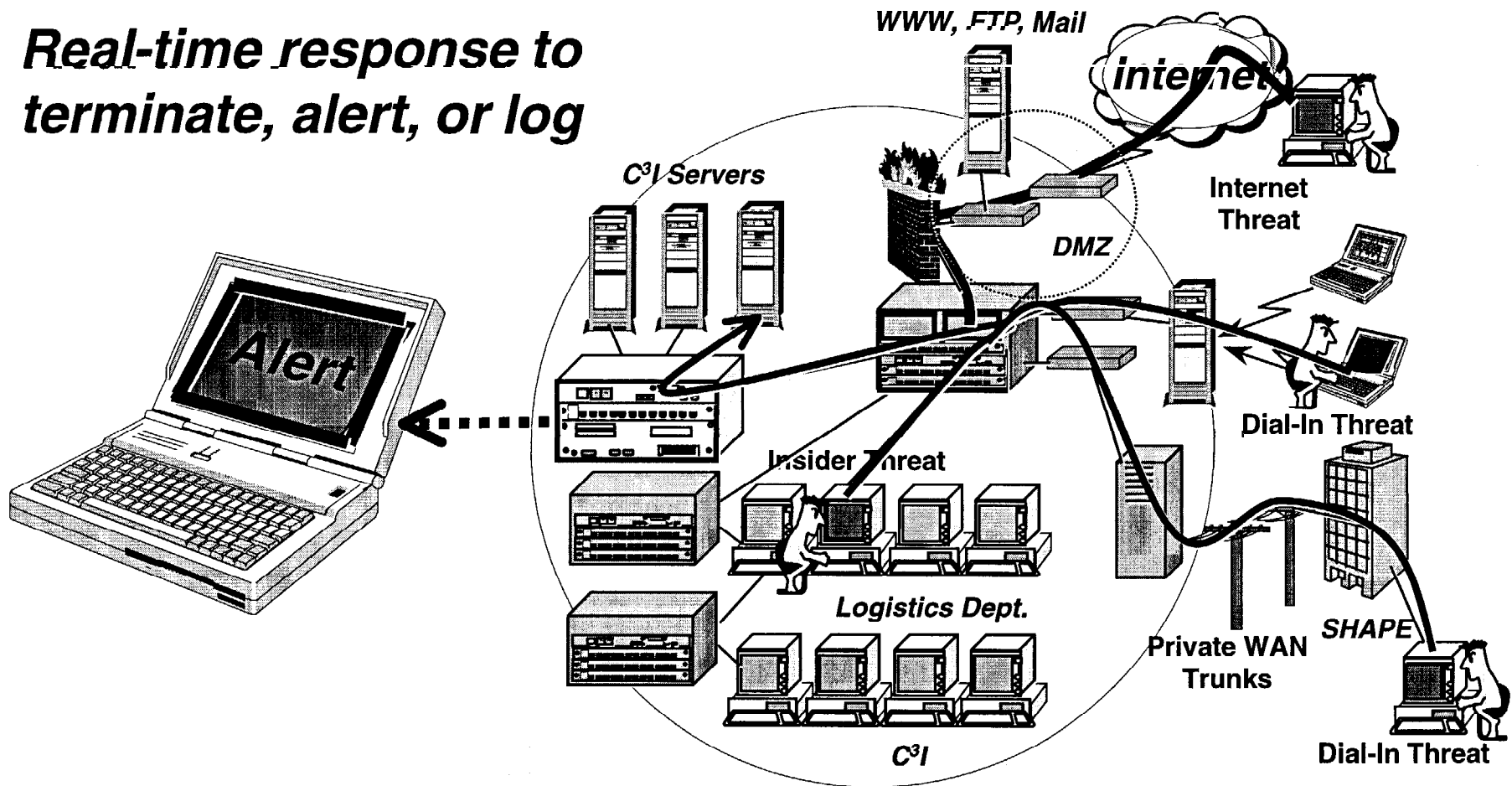
## *SecureCom Benefits*

- **Small footprint: easy deployment  
DMZ in a box, LAN in a can**
- **Any Cisco router, any Firewall, any IDS, plus all NT, Solaris, Linux, or HP/UX application**
- **multiport conditional I-way forwarding to any IDS**



# *RealSecure or NetRanger Threat Detection & Response*

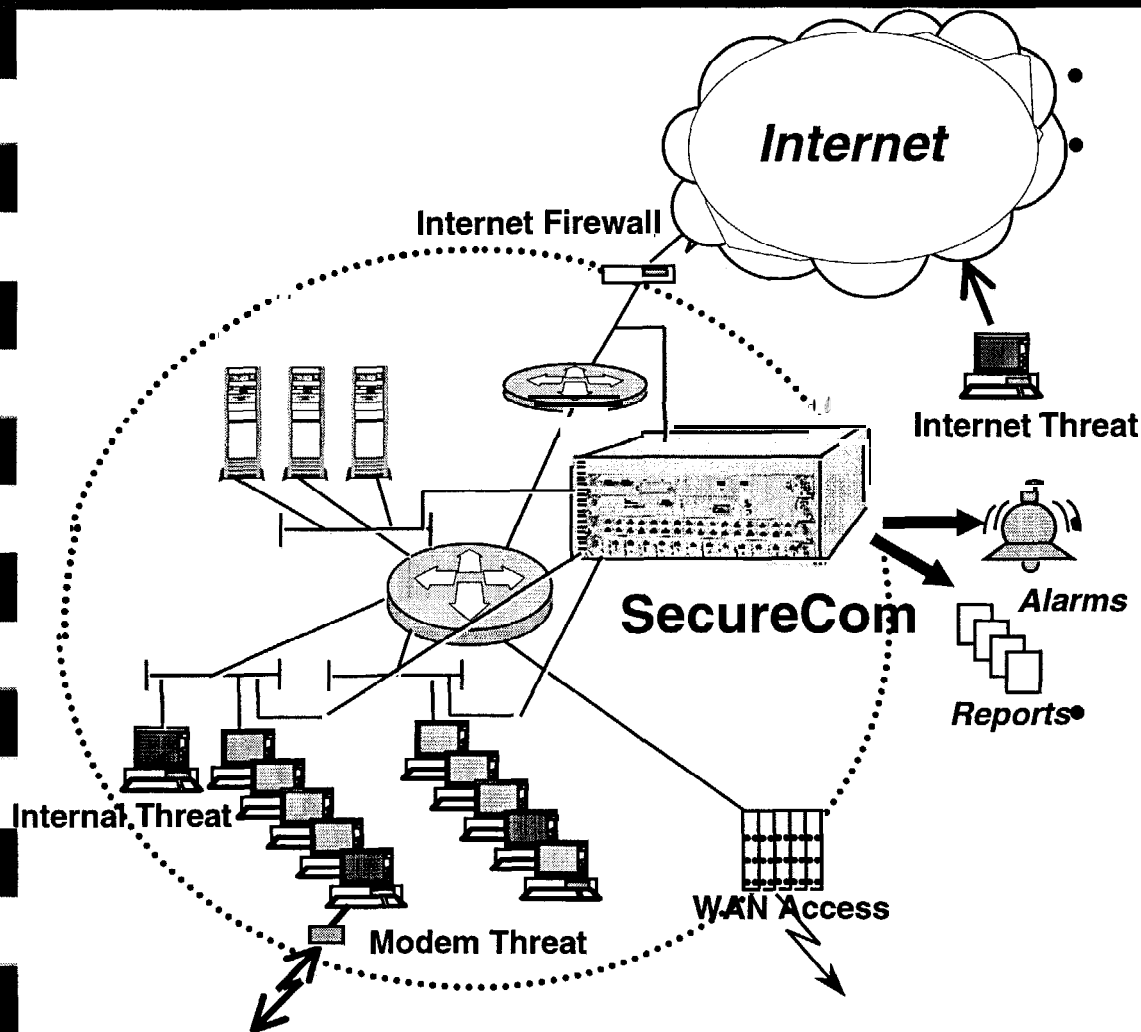
*Real-time response to  
terminate, alert, or log*



Get more for your money, monitor multiple segments with one license!



# Using the SecureCom as a multi-segment internal attack Detection System



- *Intrusion Detection*

- *Unobtrusive network security monitoring*

- Monitors data centrally
- Only one detection system is needed for multiple segments
- Cannot be detected

- *Delivers real-time security response*

- Terminates, Alerts, or Logs

- *Delivers security auditing*

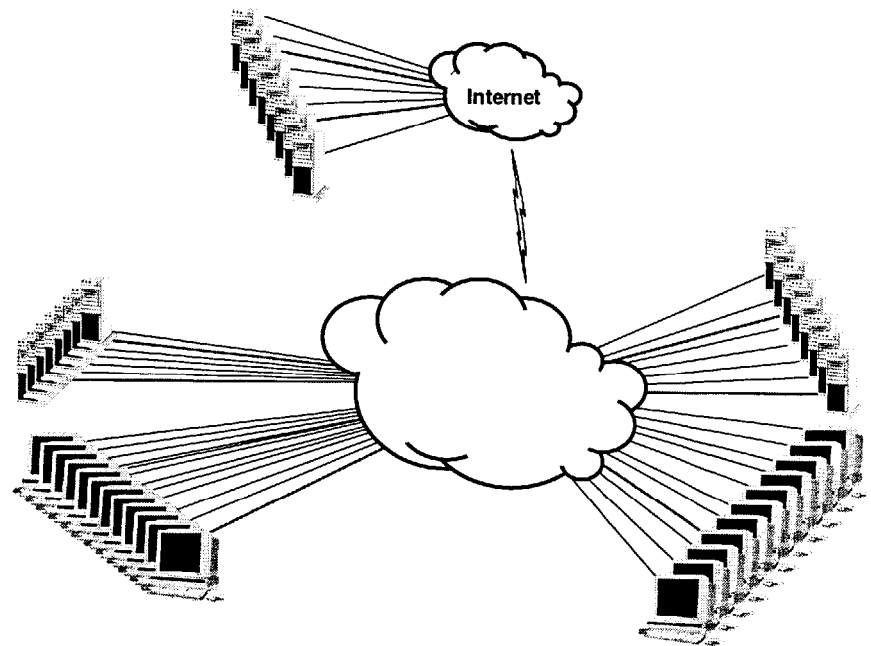
- Identifies, Alerts, & Audits workgroups



## ***Making RealSecure and NetRanger More Usable***

- **ODS multiport listening mode multiplies the number of segments monitorable by an \$8,000 or \$23,000 IDS. These prices are way to expensive to monitor every T1 circuit with a separate IDS license. Embedded with an ODS SecureSwitch, many segments may be protected by a single IDS.**
- **CMDS Enterprise is very helpful to both eliminate false alarms and develop expert profiles of user behavior.**
- **ODS conversation analysis allows the consideration of “non-attack” traffic into the mix, this is essential since both RealSecure and NetRanger are reactive only (template based detection).**

- Keeping track of who is talking to who is a good idea
  - Nature of alien conversations
    - Telnet, Rlogin, RPC, etc.
    - Non-web applications
  - Byte Symmetry
    - FTP net data outflow
    - Workstations acting as servers
  - Competitors
  - Workstation to workstation activity
    - Win 95 file sharing detection



# IP Conversation Analysis

	Src Domain	Dest Domain	Src IP	Dest IP	Server IP	SD Pkts	SD Bytes	DS Pkts
▶	SATNET	ODS-NET	4.0.1.38	10.10.75.50	10.10.75.50	3	222	2
	SATNET	ODS (DAKNET)	4.0.1.38	192.94.73.11	192.94.73.11	4	296	
	SATNET	ODS-NET	4.1.16.4	10.10.13.7	10.10.13.7	198	1959	
	SATNET	ODS (DAKNET)	4.1.16.4	192.94.73.11	192.94.73.11	5	78529	
	HP-INTERNET	ODS (DAKNET)	15.255.16.2	192.94.73.29	15.255.16.2	2563	244287	
	DEC-INTERNET	ODS-NET	16.1.0.18	10.10.13.7	16.1.0.18	175	59133	
	DEC-INTERNET	ODS-NET	16.1.0.18	10.10.100.132	10.10.100.132	1388	687324	7
	DEC-INTERNET	ODS (DAKNET)	16.1.0.18	192.94.73.11	192.94.73.11	5433	2690486	7
	DEC-INTERNET	ODS (DAKNET)	16.1.0.19	192.94.73.11	16.1.0.19	5413	2690032	
	DEC-INTERNET	ODS (DAKNET)	16.1.16.88	192.94.73.11	192.94.73.11	2	1026	
	DEC-INTERNET	ODS (DAKNET)	16.5.0.1	192.94.73.11	192.94.73.11	3	1485	
	DEC-INTERNET	ODS-NET	16.57.16.6	10.10.100.132	10.10.100.132	4	641	
	APPLE-WWW	ODS (DAKNET)	17.254.0.50	192.94.73.11	192.94.73.11	237	38750	
	MIT	ODS-NET	18.52.0.20	10.10.13.138	10.10.13.138	4	721	
	MIT	ODS-NET	18.52.0.20	10.10.24.35	18.52.0.20	39217	22188157	
	MIT	ODS (DAKNET)	18.71.0.151	192.94.73.11	192.94.73.11	243	45181	1
	MIT	ODS-NET	18.71.0.151	10.10.13.7	10.10.13.7	4	10665	
	MIT	ODS (DAKNET)	18.71.0.151	192.94.73.11	192.94.73.11	175	36650	
	MIT	ODS-NET	18.71.0.151	10.10.13.138	10.10.13.138	8	1947	7
	MIT	ODS-NET	18.224.0.151	10.10.13.138	18.224.0.151	20	16617	
	MIT	ODS-NET	18.224.0.151	10.10.13.138	18.224.0.151	29	13488	
	MIT	ODS (DAKNET)	18.224.0.151	192.94.73.11	192.94.73.11	2	164	
	CSC	ODS (DAKNET)	20.7.1.97	192.94.73.29	20.7.1.97	4	256	
	CSC	ODS (DAKNET)	20.7.1.97	192.94.73.29	192.94.73.29	4	256	
	ATHOME	ODS (DAKNET)	24.3.89.76	192.94.73.29	24.3.89.76	1390	127614	

**Which Device is "Server"**

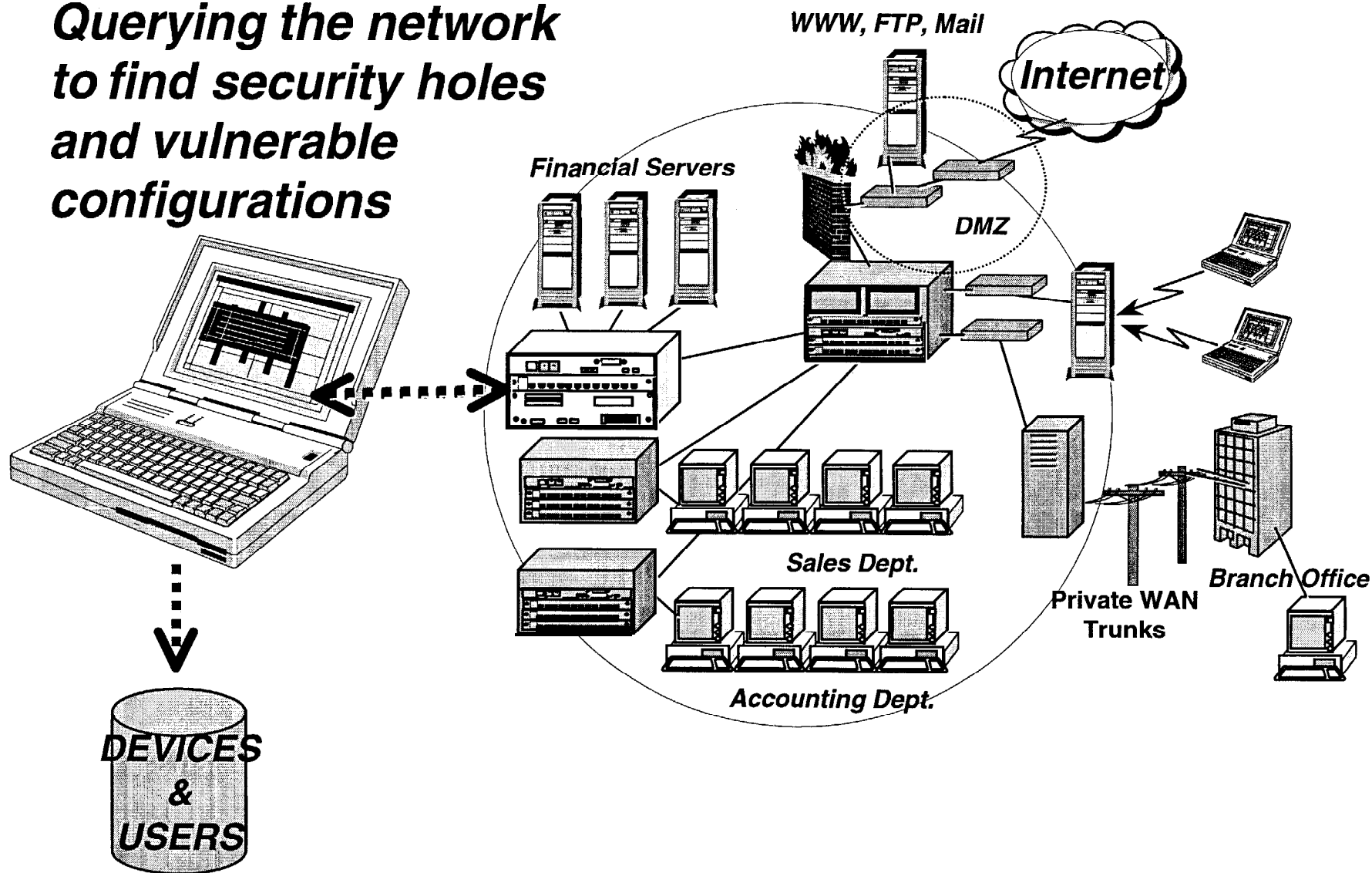
**Source IP Address  
and Domain Name**

**Destination IP Address**

**Reveals Who is Talking to Whom  
& What They Are Doing**

# Internal Network Monitoring with SNMP/RMON

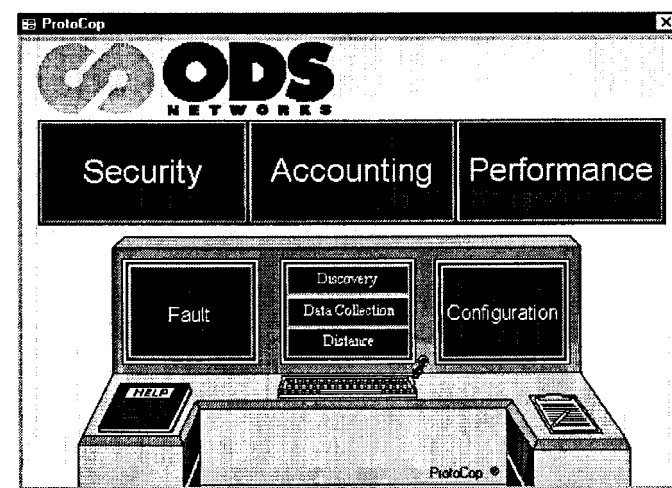
*Querying the network  
to find security holes  
and vulnerable  
configurations*





## *All 5 ISO Network Management Categories*

- **Data-centric, not device-centric management**
  - Delivers network inventory
  - Collects data from any SNMP-managed device
  - Identifies problems by category regardless of device brand, type or location
  - Provides standard & customizable reporting on collected data
    - Security
    - Configuration
    - Fault
    - Performance
    - Accounting





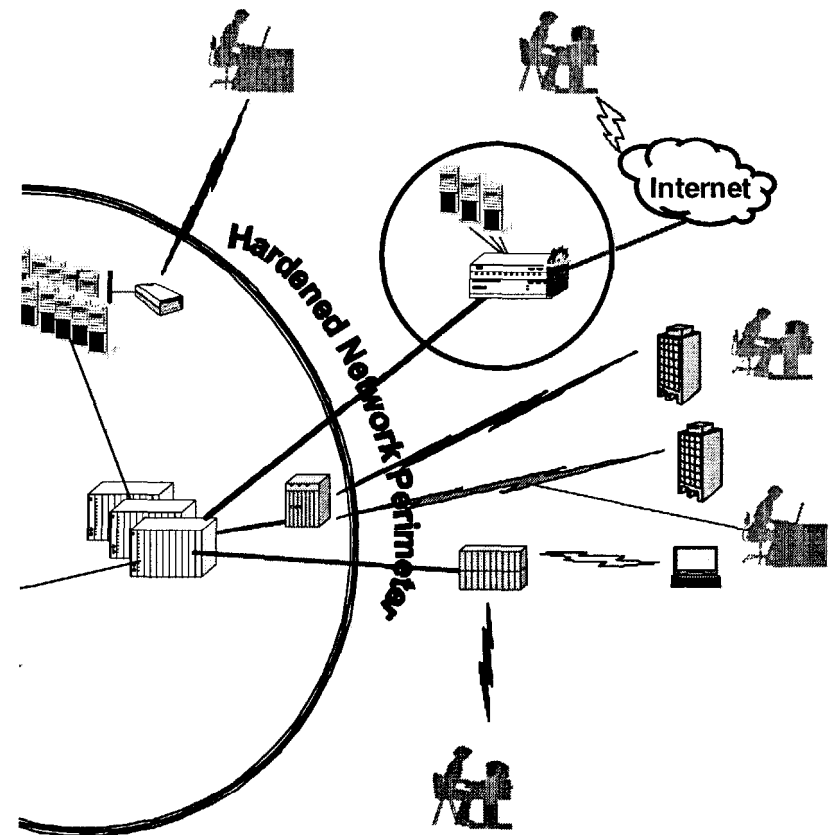


## *Elements of a Layered Defense*

- **External Threats:**
  - Screening Router
  - Auditing of DMZ assets: Mail, Web, FTP
  - Firewall plus IDS
  - Authenticated remote users - VPN, defense against cryptographic attacks and traffic analysis
  - Firewall and VPN leak detection, audit, and user profiling
  - Back door detection
- **Internal Threats:**
  - Internal IDS
  - Protection against clever VPN attacks: spoof, twin, theft, bandwidth, replay, cryptographic, traffic analysis
  - Network Conversation analysis
  - Host conversation analysis
  - Internal authentication, compartmentalization \*
  - Using existing, rich data sources: logs from routers, switches, hosts, workstations
  - Security policy audit and enforcement
  - Statistical behavior analysis for habit changes from norm
  - Users compared to group bell curves: The Ames detector

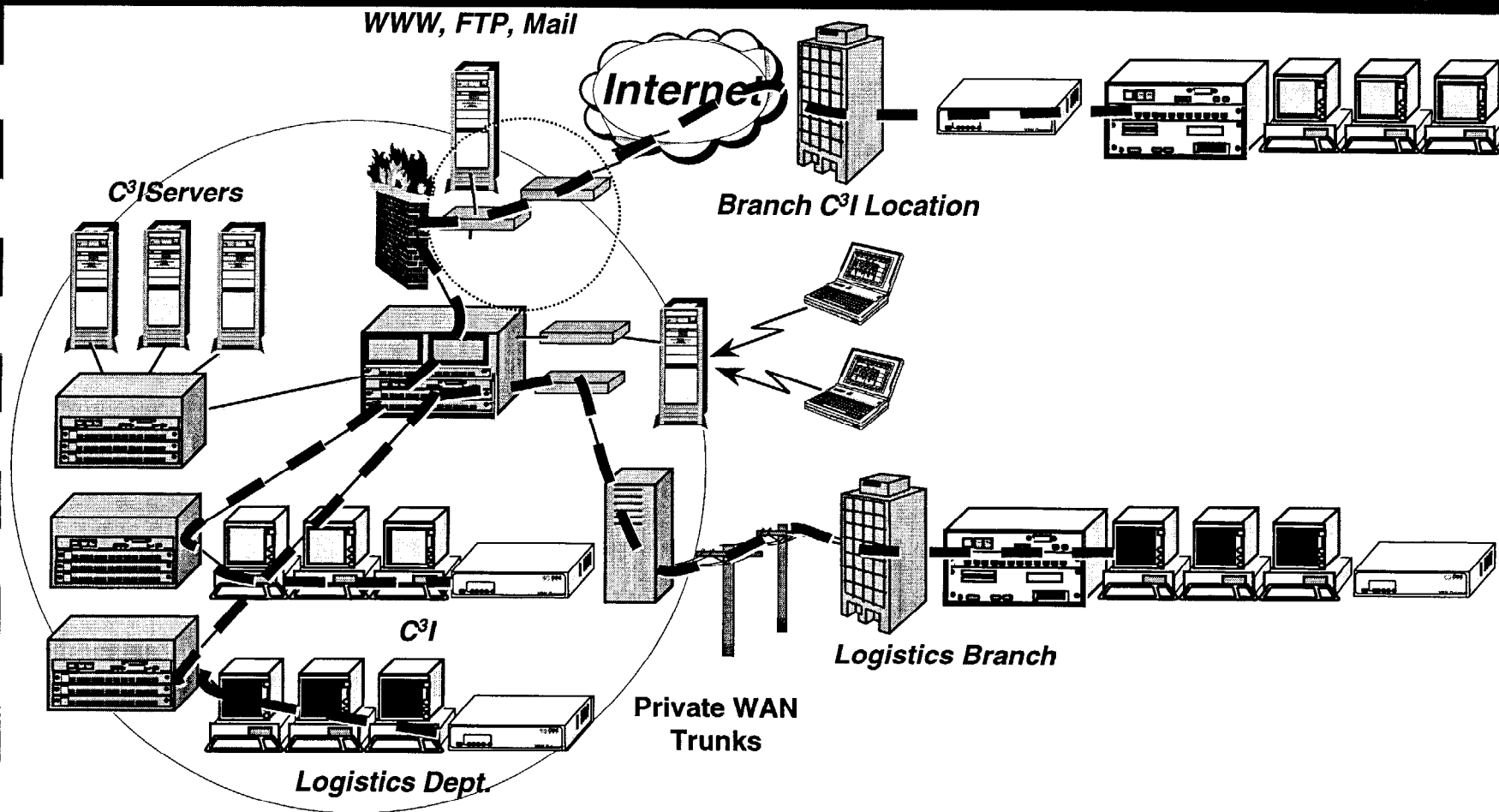
# *Hardening the non-existent Perimeter*

- We all know more than a firewall is necessary
- Deploy:
  - Host OS-based monitoring
  - Application-based monitoring
    - Web, SMTP, FTP, Firewall
  - Router log analysis
  - Modem back door protection
  - IDS on WAN and RAS links
  - Two-factor crypto authentication
    - Strong crypto over the Internet
    - Cross compartment authentication



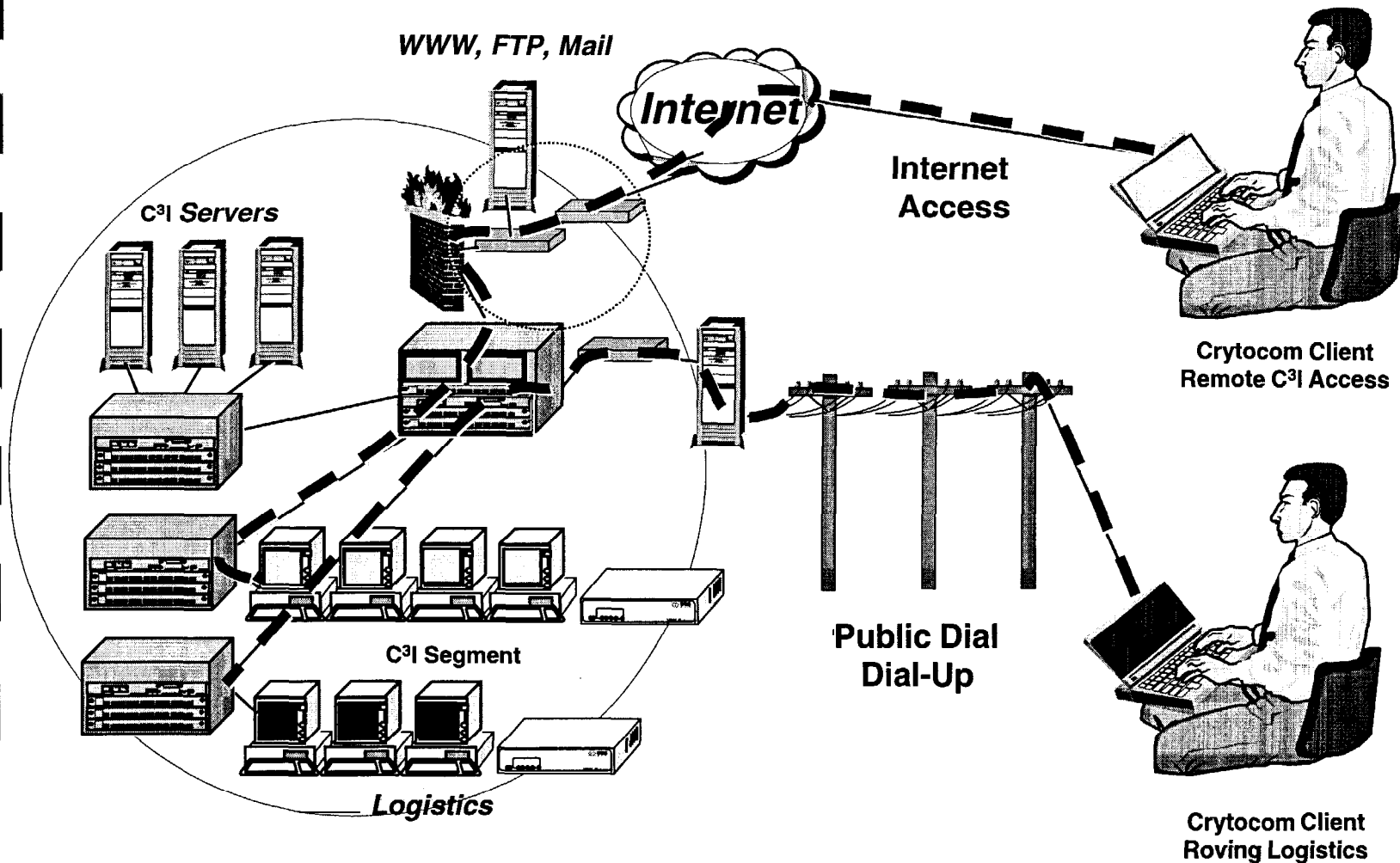


# Protect, Compress, Eliminate Your Expensive WAN Trunks





# *The Remote User: Per Packet Authentication, Ames/duress Detection too!*





## **Competitive Generalizations**

- Most “remote access” products are for dial-up and/or are media dependent.
- Most of their security features are limited to weak authentication (of the user) upon first part of connection only.
- Very few support “home network” configuration. (Key to back door detection.)
- Serious security flaws. Lacking: Salt values, hardware key generation, sequence numbers as additional salt to prevent replay.
- Most VPN solutions are not designed for resistance against serious enemies.



## ***What strengths does CryptoWatch have?***

- **1024 bit RSA signatures of SHA-1 or MD5**
- **Idiot proof operation**
- **IDEA, Triple DES, and new keys every 60 seconds.**
- **Low cost**
- **Works across any WAN, dial, ISDN, FR, X.25, ADSL ,...**
- **Works on any LAN,**
- **Built in compression, pre-encryption...**
- **Approvals and history in compartmentalized environments.**
- **Export approval for strong crypto without key escrow, key recovery, or the need for prior export licenses to customers in 44 countries.**

- **Network Data**

- Provides a Network Perspective
- Cannot identify what happened - host state awareness lacking
- Is rendered less useful when encrypted
- Is essential to prove any case - non-repudiation requires trace

- **Host Data**

- Provides exact log of what happened
- Tracks Who, What & When
- Cannot Identify Where a User really is
- Is the richest source of data and is still completely useful for monitoring criminal use of encrypted communications



**Integration provides a common view of suspicious traffic & corresponding illegal user activity**

## *Computer Misuse Detection System*



Intrusion Detection

Data Forensics

Audit Management



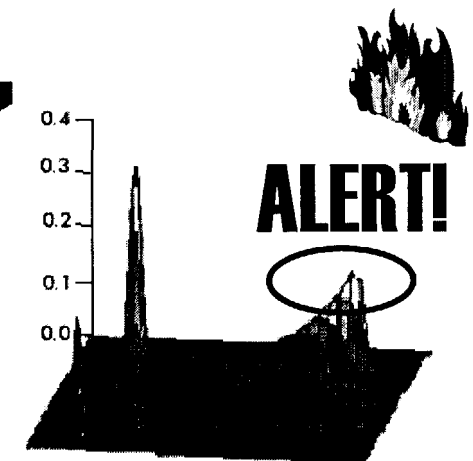
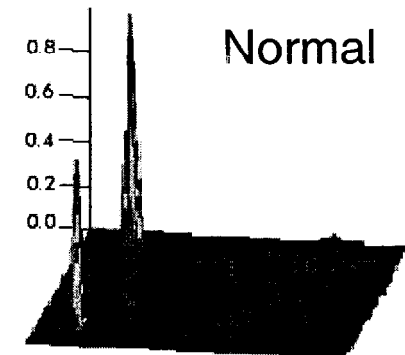
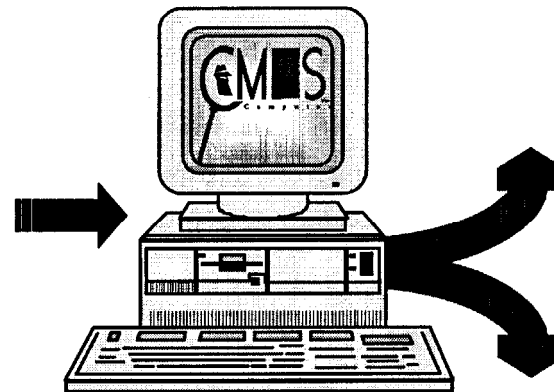


## *Internal Audit, Data Rollup, then Proper Security Response*

- Numerous inputs can be consolidated into a single management console
  - Intrusion Detection Systems
  - Firewalls
  - Host monitoring
  - Database access
  - Application logs
  - Authentication
  - Dial-up access
- Response(s) can be automated based on enterprise correlation

# Bringing it All Together Enterprise Security Console

- How to deal with the data issue:
- Megabytes generated everyday
- Large audit reduction requirement
- “Normalizing” the data across disparate systems
  - Log files - OS, Firewalls, applications, RAS
  - Network infrastructure
  - Conversations
  - Behavioral anomalies
- Constant Change



As a user works, CMDS automatically builds a histogram of the user's normal activity, then alerts on any change...

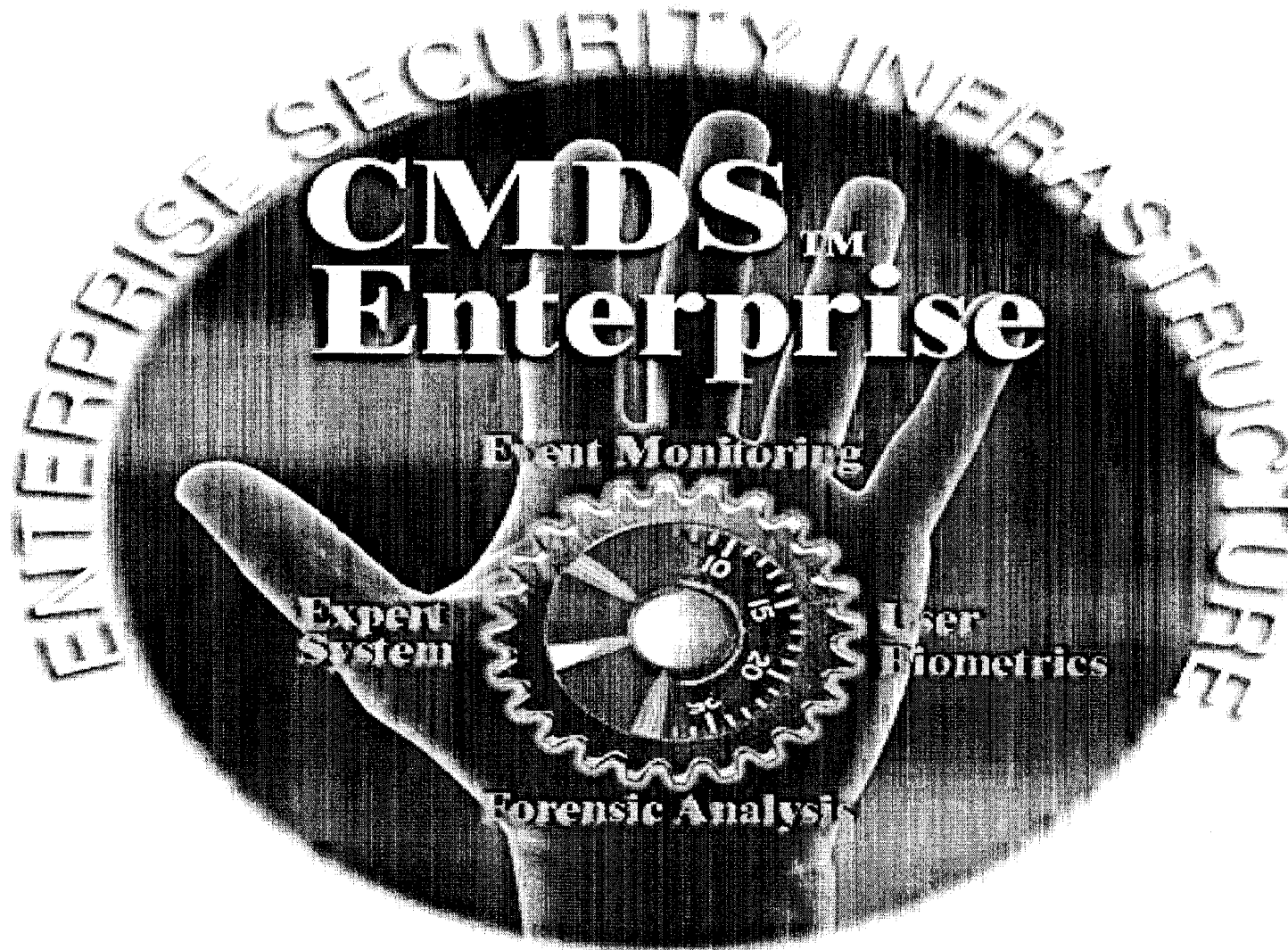
- **CMDS correlates individual alerts and data**
- **Use relational database to store the data**
  - Event-based schema
  - Use statistical behavioral profiling
- **OLAP On-Line Analytical Processing**
  - Allows analysis of very large data sets - correlation by:
    - Date/Time
    - Type of event
    - Location of event
    - Severity of event
    - Trend analysis
    - Modeling and prediction

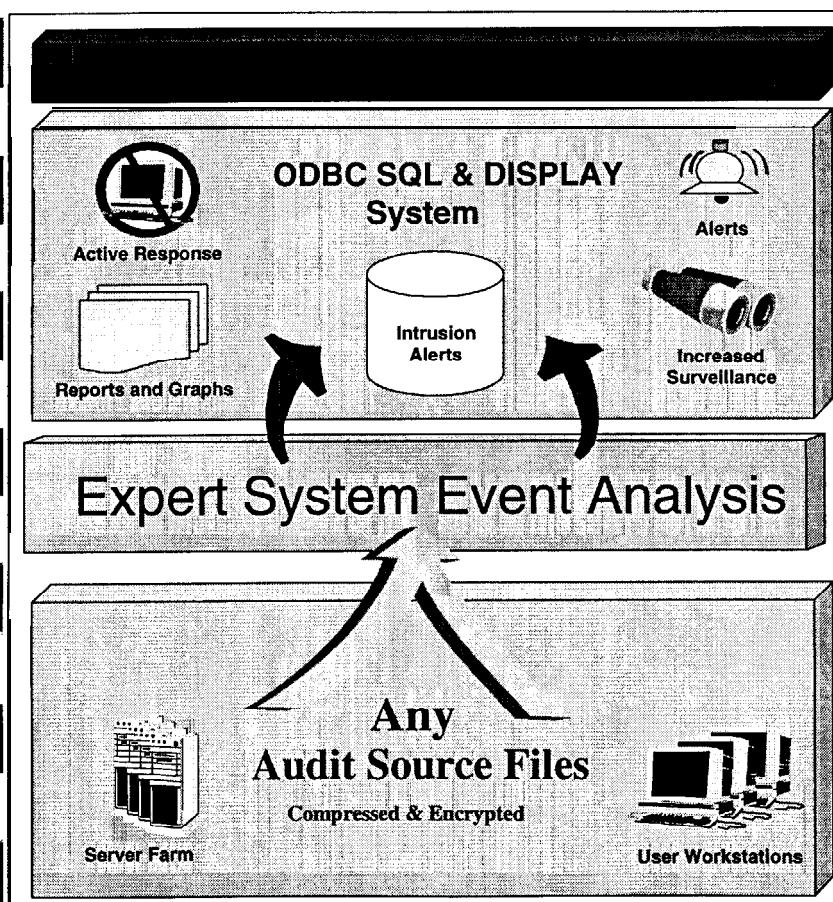




## ***The Expert Security Solution***

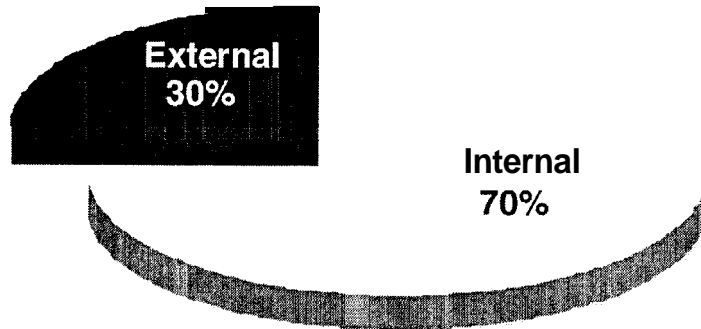
- **Real Security Expertise is Rare**
  - Too many issues, too few wizards
  - Critical mass issues, cost sharing of wizards
- **Phased awareness**
  - Initial requests for 2% problems: firewalls, IDS, VPN
  - 90% Solutions:  
Solving the insider problem, fraud, theft, and the like.
- **Layered defenses are best.**
- **A wealth of security violation data lies dormant in your network, sometimes collected, but never methodically analyzed except after a major embarrassment.**
- **A Security Expert System is required to simplify the problem and perform the necessary data reduction, correlation, and isolation of security problems.**





- CMDS is an expert system that monitors internal events in organizational Network(s).
- Currently monitors NT OS Audit Logs:
  - Impossible to do job manually
- Configurable to monitor events from:
  - Critical Applications
  - SQL DBMS'
  - Any Pertinent Data Sources
- a Pro-active approach to security policy generation and management

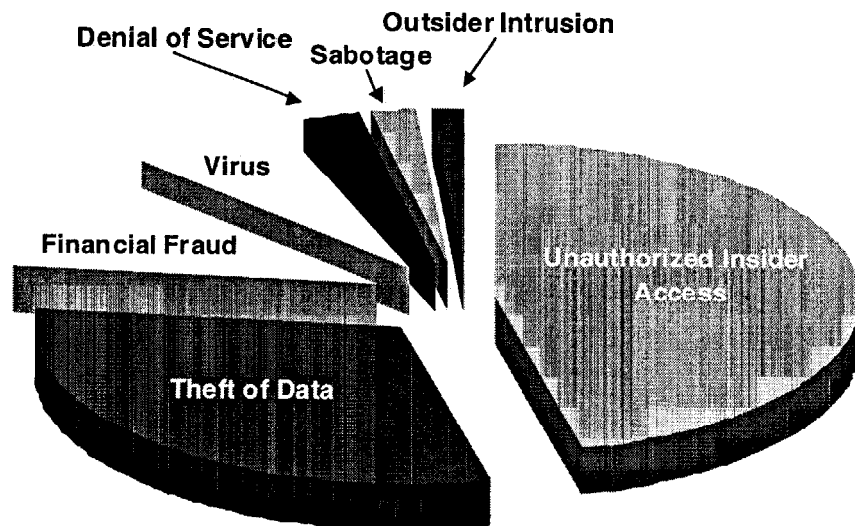
# Why CMDS<sup>tm</sup> Enterprise??



- Percentage of losses for computer and network security events by cause:

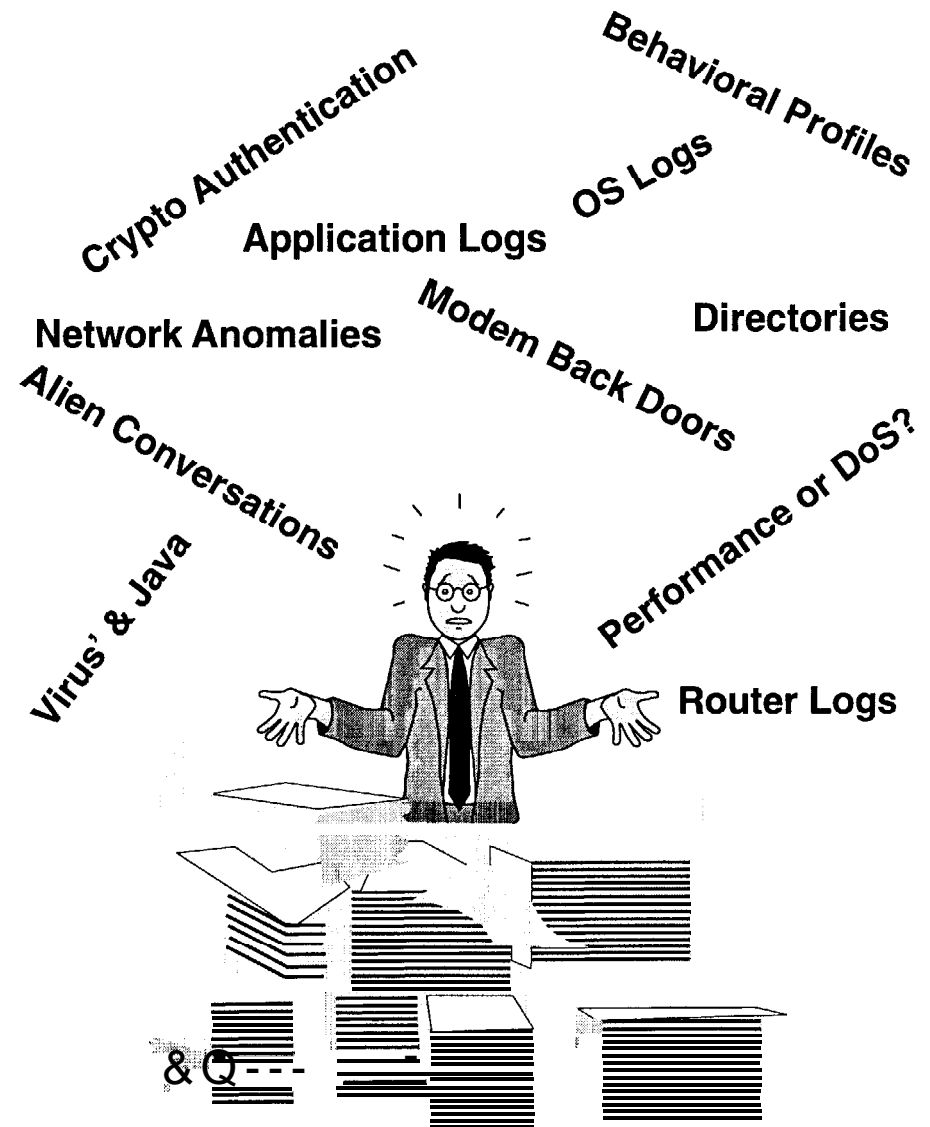
- 46% insider misuse
- 32% data theft
- 11% financial fraud
- 7% virus attacks
- 2% sabotage
- 2% outsider penetration

- 70% of security events are by insiders
- Our networks have a hard, crunchy exterior with a soft, squishy interior
- Most security expenditures attempt to solve the wrong problem



# Problems Security Professionals Face Every Day

- Sifting through the massive amount of data quickly to find:
  - Patterns,
  - Anomalies or
  - Other indications of intrusions or attacks
- With CMDStm Enterprise, security officer's will be able to:
  - focus proactively on security policy management instead of auditing system event logs







# ***CMDS<sup>tm</sup> Enterprise Provides:***

- **Open Architecture**
  - Supports standard SQL databases
  - Flexible and Extensible
- **Highly Scalable Architecture**
- **User Behavior Fingerprinting**
- **Expert System for Security Policy monitoring**
- **Universal Audit Parsing Interface**
- **Centralized Audit Management**



# ***CMDStm Enterprise Services***

**CMDStm Enterprise was designed to support the following services:**

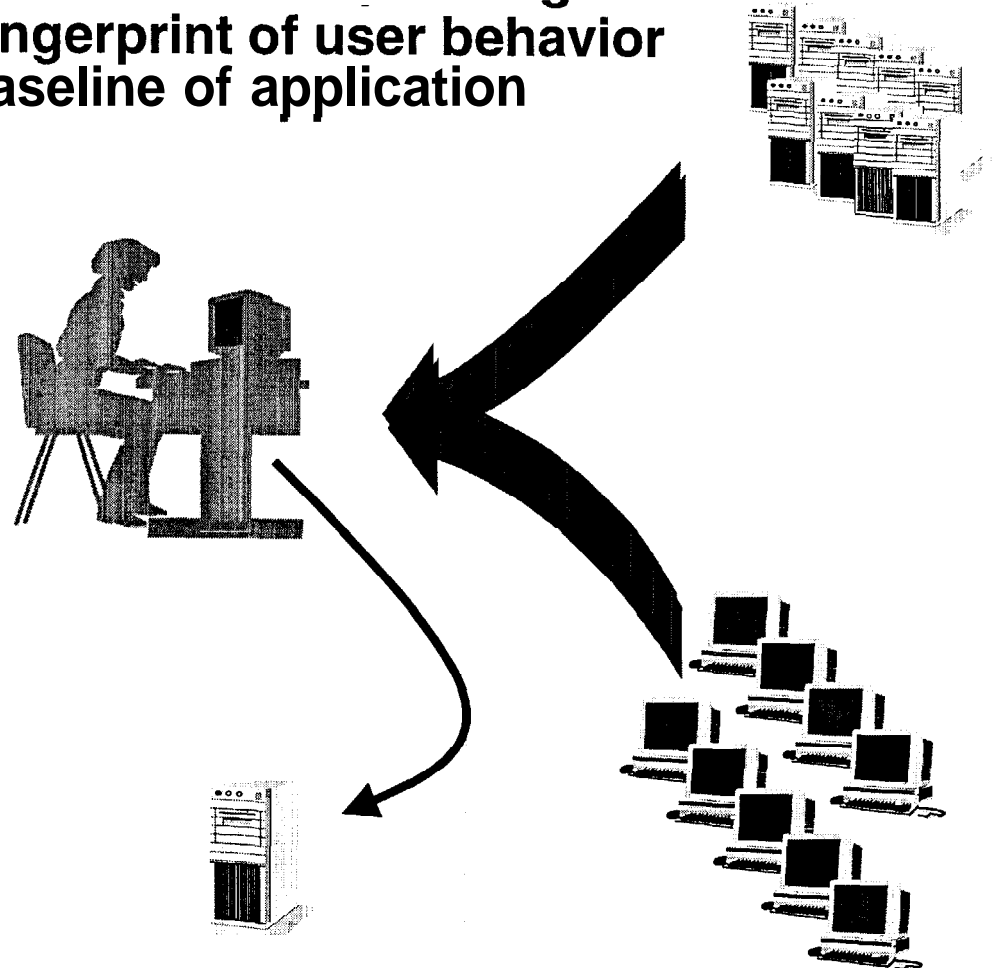
- **Collection of operational audit from hosts and event data from any other system within the organization**
- **Encryption and reduction of operational audit when transmitted across the network**
- **Reformatting and parsing of virtually any audit source for event analysis**
- **Audit data log filtering**
- **Expert system analysis of filtered event logs for signs of known intrusions and attacks**
- **Behavioral and statistical profiling of definable categories for all users**



# ***CMDS<sub>tm</sub> Enterprise Services (CONT'D)***

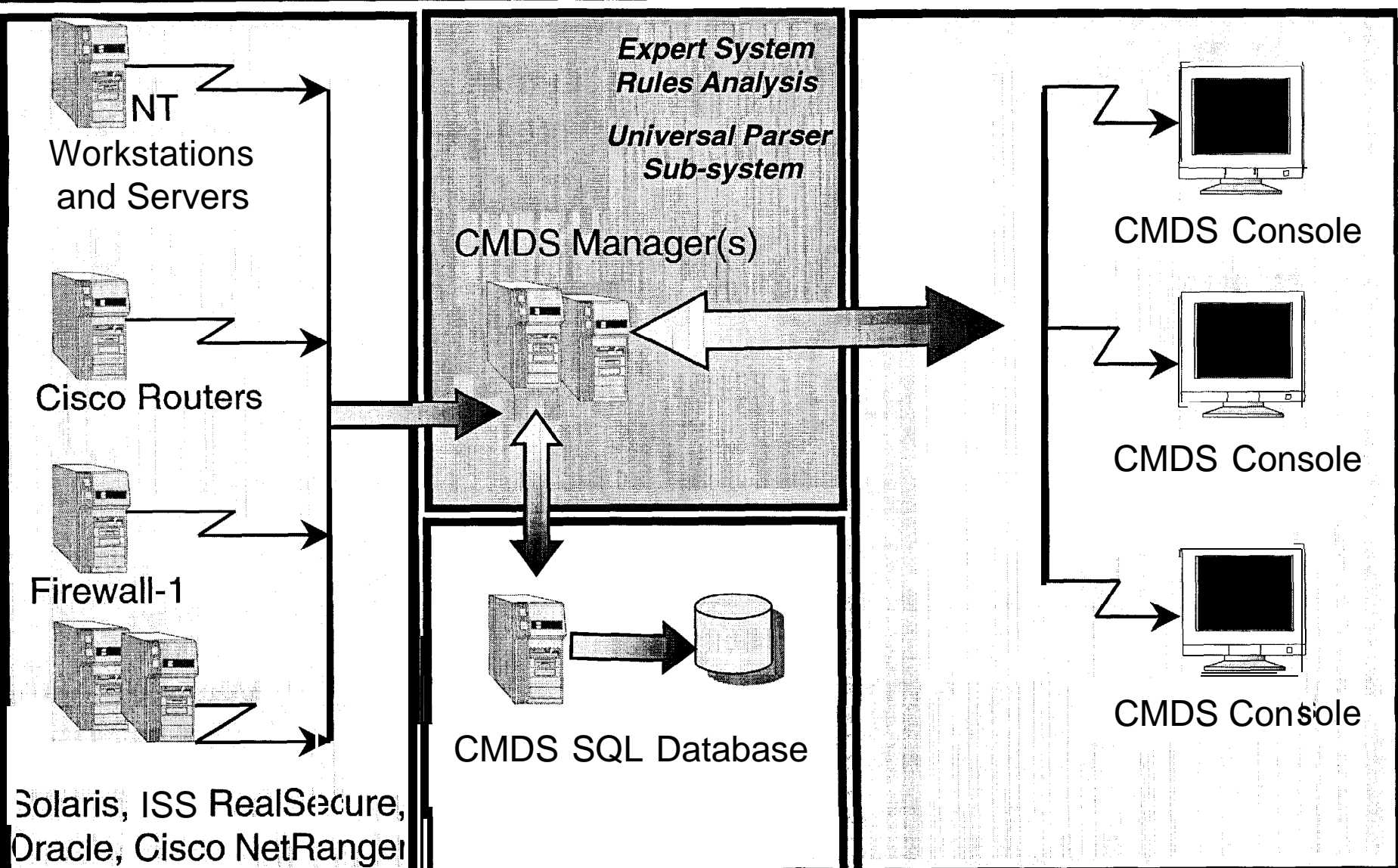
- SQL Database repository, includes management and maintenance
- Severity level classification, 0 - 5
- Generation of warnings, alerts
- Notification through pagers, email, Managers of Managers
- Command and Control through notification scripting
- *Ad hoc* query, filtering and sorting of event data
- Reporting and Charting
- Centralized audit management, includes archival and retrieval

- **CMDStm Enterprise's Integrated statistical profiling engine dynamically builds a fingerprint of user behavior and automatically creates a baseline of application operations.**
- **Every user settles into an usage pattern over time**
- **CMDStm Enterprise detects when that pattern changes**
  - Accesses to servers
  - Accesses to workstations
  - File Browsing
  - Nighttime activity
  - Peer group analysis





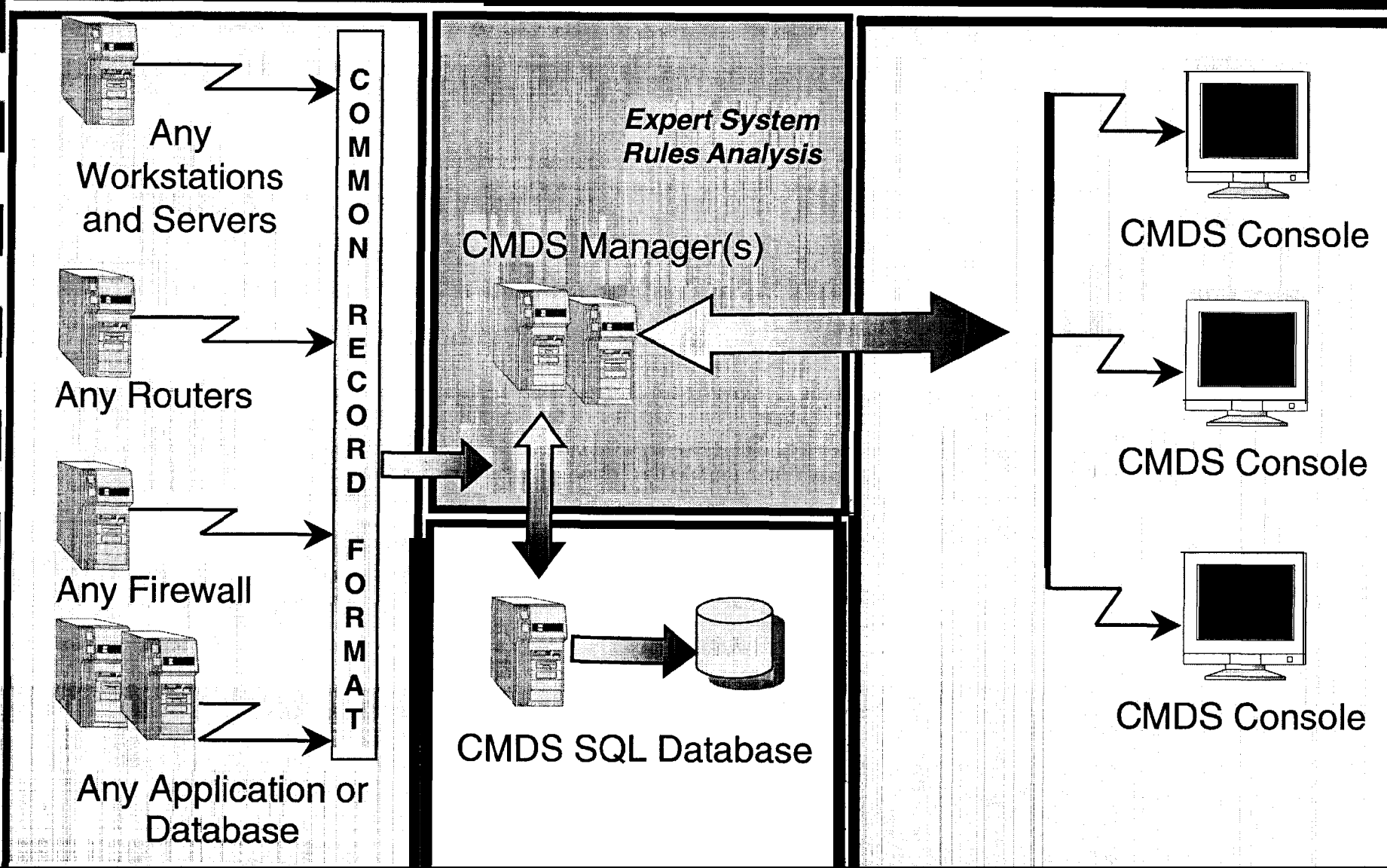
# ***CMDS<sup>tm</sup> Enterprise Architecture***

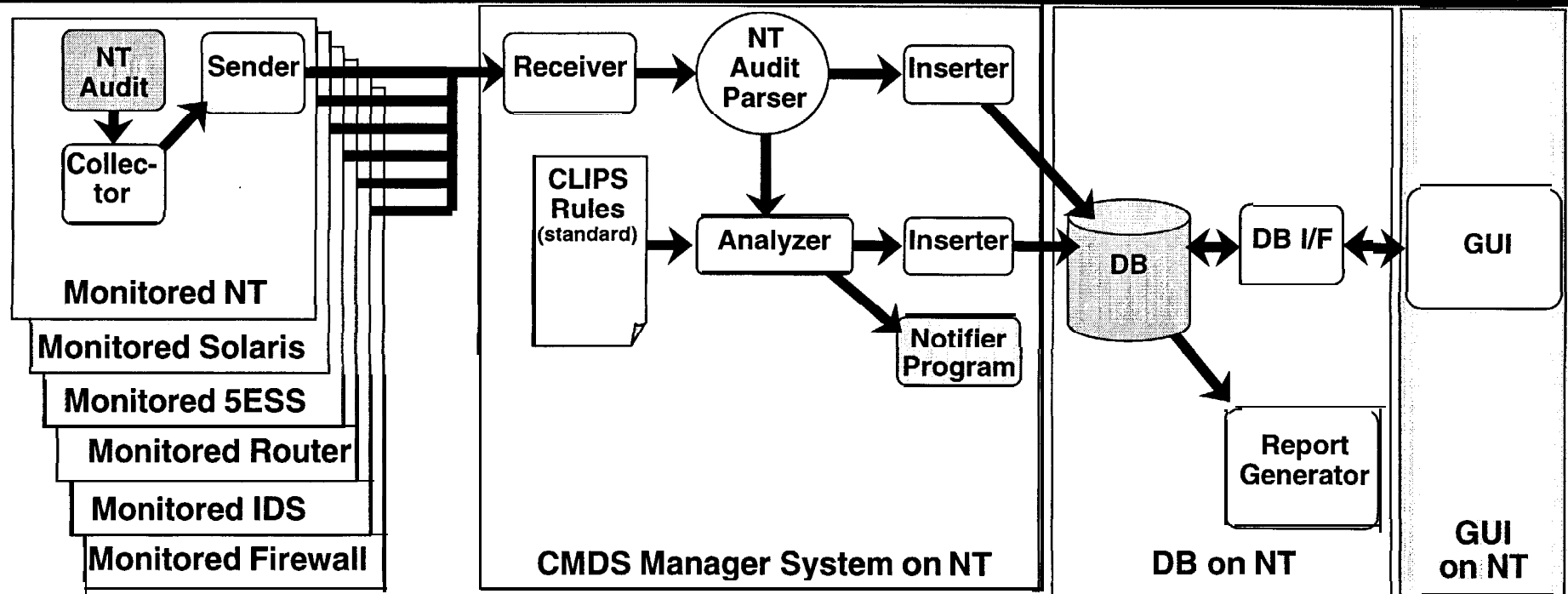




## *CMDStm Enterprise Architecture (cont'd)*

# *Universal Parser Sub-System*

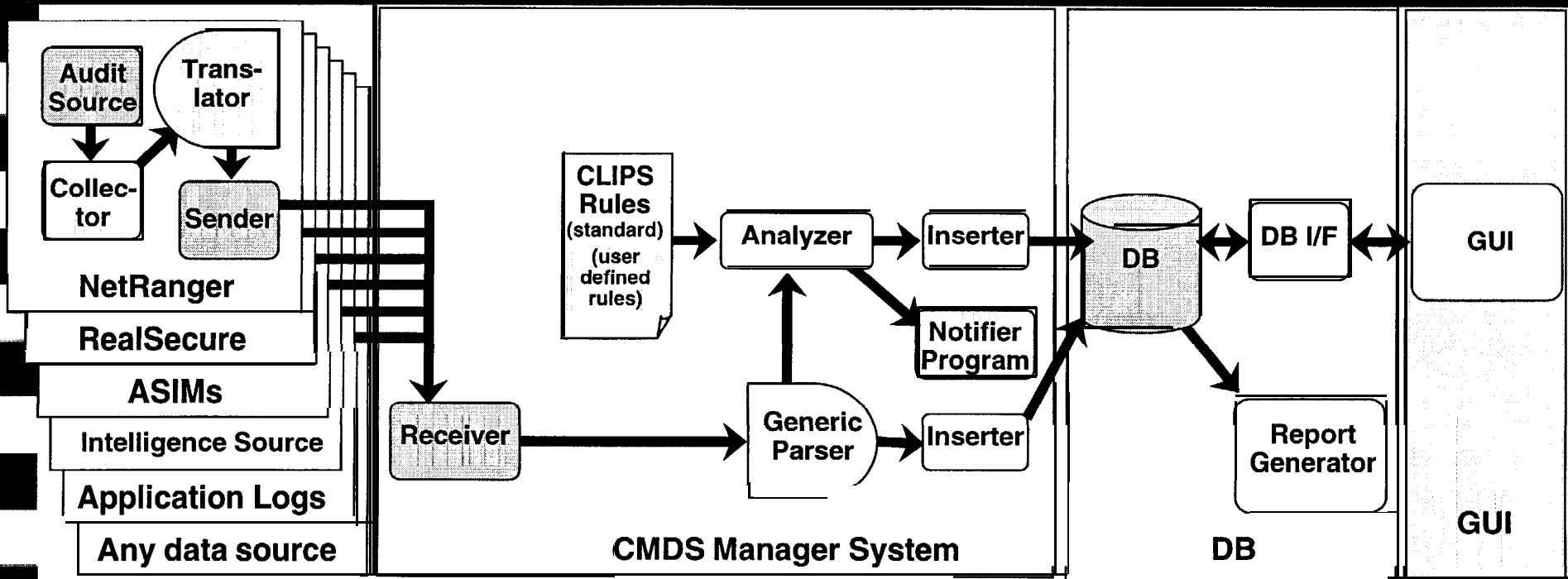




## Highlights:









- Multiple agents are monitored by a single CMDS Manager system
- Expert System Rules find standard problems
- Activity profiler finds exceptions to each person's historical usage patterns
- A criminal may fit his own historical pattern, but will stand out as a group behavioral exception.

# Universal Parser Process



## Highlights:

- Translator on the client side reduces workload of the CMDS Management system
- Collector and Translator may be combined as a single process

	Provided in CMDS 4.0		Direct reading of file by opening
	User Developed		Files transferred by directory
	3rd Party Vendor Developed		ODBC Interface
			CORBA Interface
			Secure CORBA using SSL



## Event Log

Log Data Help

Unacknowledged Event Status

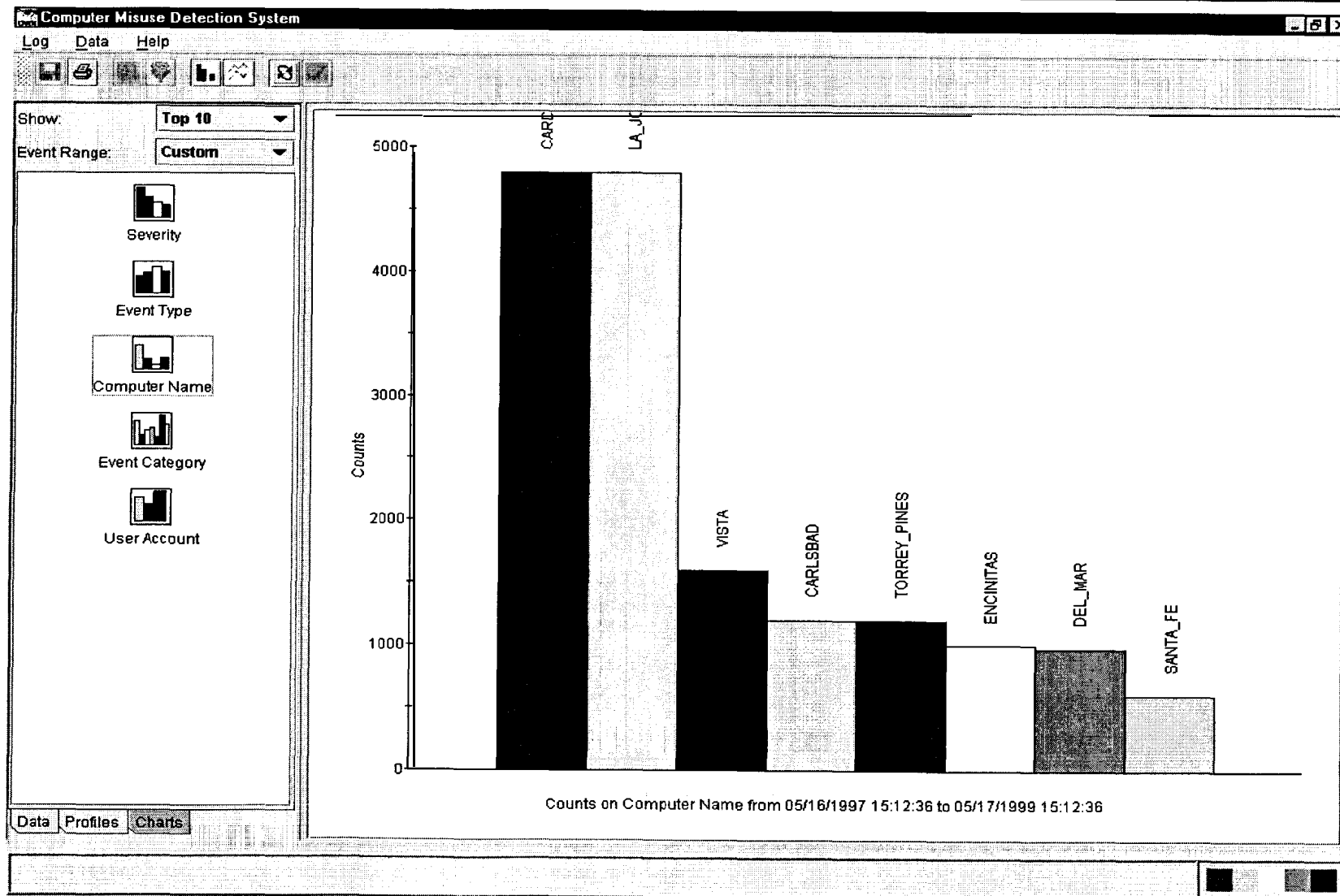
- 5 Network
  - 5 West Coast
    - 5 Products&Sales
      - 2 CARDIFF
      - 3 CARLSBAD
      - 5 DEL-MAR
      - 4 ENCINITAS
      - 2 LA\_JOLLA
      - 0 SANTA-FE
      - 3 TORREY-PINES
      - 1 VISTA

**Event Log**

	Time Generated	Severity	Operating System	Event Number	Event Type	User Name	Computer Name	Ev
1	1999-01-25 15:29:42.000	3	nt	535	passed	Heather	TORREY_PINES	log
2	1999-01-25 15:29:42.000	3	nt	627	passed	Heather	TORREY_PINES	acc
3	1999-01-25 15:29:42.000	3	nt	625	passed	Heather	TORREY_PINES	acc
4	1999-01-25 15:29:42.000	3	nt	625	passed	Heather	TORREY_PINES	acc
5	1999-01-25 15:29:42.000	3	nt	639	passed	Heather	TORREY_PINES	acc
6	1999-01-25 15:29:42.000	3	nt	641	passed	Heather	TORREY_PINES	acc
7	1999-01-25 15:29:36.000	3	nt	535	passed	George	TORREY_PINES	log
8	1999-01-25 15:29:36.000	3	nt	627	passed	George	TORREY_PINES	acc
9	1999-01-25 15:29:36.000	3	nt	629	passed	George	TORREY_PINES	acc
10	1999-01-25 15:29:36.000	3	nt	625	passed	George	TORREY_PINES	acc
11	1999-01-25 15:29:36.000	3	nt	639	passed	George	TORREY_PINES	acc
12	1999-01-25 15:29:36.000	3	nt	641	passed	George	TORREY_PINES	acc
13	1999-01-25 15:29:30.000	3	nt	535	passed	Frank	TORREY_PINES	log
14	1999-01-25 15:29:30.000	3	nt	627	passed	Frank	TORREY_PINES	acc
15	1999-01-25 15:29:30.000	3	nt	629	passed	Frank	TORREY_PINES	acc
16	1999-01-25 15:29:30.000	3	nt	625	passed	Frank	TORREY_PINES	acc
17	1999-01-25 15:29:30.000	3	nt	639	passed	Frank	TORREY_PINES	acc
18	1999-01-25 15:29:30.000	3	nt	641	passed	Frank	TORREY_PINES	acc
19	1999-01-25 15:29:24.000	3	nt	535	passed	Elizabeth	TORREY_PINES	log
20	1999-01-25 15:29:24.000	3	nt	627	passed	Elizabeth	TORREY_PINES	acc
21	1999-01-25 15:29:24.000	3	nt	629	passed	Elizabeth	TORREY_PINES	acc
22	1999-01-25 15:29:24.000	3	nt	625	passed	Elizabeth	TORREY_PINES	acc
23	1999-01-25 15:29:24.000	3	nt	639	passed	Elizabeth	TORREY_PINES	acc
24	1999-01-25 15:29:24.000	3	nt	641	passed	Elizabeth	TORREY_PINES	acc
25	1999-01-25 15:29:18.000	3	nt	535	passed	Danny	TORREY_PINES	log
26	1999-01-25 15:29:18.000	3	nt	627	passed	Danny	TORREY_PINES	acc
27	1999-01-25 15:29:18.000	3	nt	629	passed	Danny	TORREY_PINES	acc
28	1999-01-25 15:29:18.000	3	nt	625	passed	Danny	TORREY_PINES	acc
29	1999-01-25 15:29:18.000	3	nt	639	passed	Danny	TORREY_PINES	acc
30	1999-01-25 15:29:18.000	3	nt	641	passed	Danny	TORREY_PINES	acc

Data Profiles Charts

There are 16100 records in the result set. 500 record(s) loaded.





## ***CMDStm Enterprise Reports***

**Alerts and Warnings by Machine Name**

**Alerts and Warnings by Event Type**

**Alerts and Warnings by User Name**

**Alerts and Warnings by Day**

**Alerts and Warnings by Week**

**Failed Directory/Failed Access by Machine Name**

**Failed Logins by Machine Name**



## *Where CMDS Is Used Worldwide*



### **U.S. Government**

**US. Federal Agencies**

**U.S. Department of Defense**

### **Foreign Countries**

**European Governments**

**NATO**

### **Pacific Rim Countries**

**Australian Government**

**Japanese Government**

### **U.S. Commercial Organizations**

**Telecommunications**

**Software Design Organizations**

**Financial Organizations**



# CMDS in Action

**CAST: Alice: - Manager, Computer Security Officer: - Security, Kurt: - Disgruntled employee, Building Security**

CMDS constantly monitors all activity for telltale signs of illegal activity...

CMDS Alerts on the Hacker Attack and to the Privilege upgrade. Security obtains detailed analysis.

CMDS Alerts on Tagged User "Guest". Security calls Building Security and notifies them of the situation.

Building Security goes to Alice's office and catch Kurt in the act of stealing personnel information!

Building Security contact Security of the arrest and prepares a CMDS report of the event trail for prosecution.

11:00 AM

Time Line

11:45 AM

Alice leaves for lunch, but forgets to lock her workstation.

11:57 AM

Shortly after leaving her office, Kurt enters Alice's office with a utility that will give him root access to Alice's machine.

11:59 AM

Then Kurt runs the User Manager to unlock the Guest account; grants Guest Admin privileges with a new password; removes Admin upgrade trail to cover his tracks and removes floppy. Kurt returns to his office.

12:02 PM

5:04 PM

Alice leaves for home.

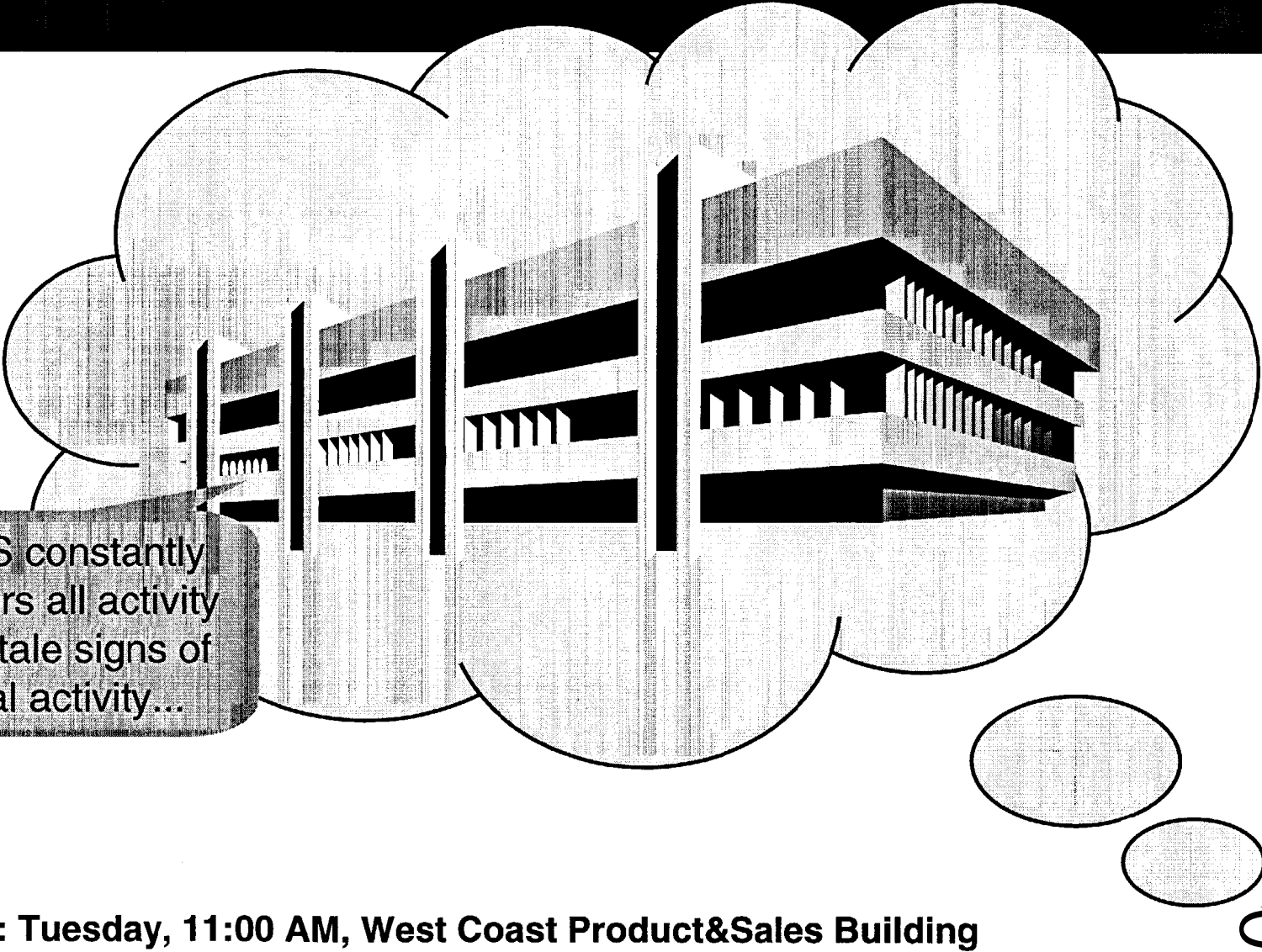
5:34 PM

At the end of the day Alice leaves for home, only to have Kurt enter her office and begin downloading sensitive data...

5:38 PM

5:49 PM

6:56 PM



CMDS constantly  
monitors all activity  
for telltale signs of  
illegal activity...

**DateLine: Tuesday, 11:00 AM, West Coast Product&Sales Building**



Computer Misuse Detection System

Log Data Help

Refresh

Sort...

Filter...

Acknowledge...

Remove Filter/Sort

Preferences...

- ☐ 0 DEL\_MAR
- ☐ 3 ENCINITAS
- ☒ 5 LA\_JOLLA
- ☐ 3 SANTA\_FE
- ☐ 1 SANTE\_FE
- ☐ 4 TORREY\_PINES
- ☐ 5 VISTA

	Time (GMT-0800)	Severity	Operating System	Event Number	Event Type	User Name	Computer Name	Ev
1	1999-01-15 11:06:58.000	5	nt	534	passed	Alice	LA_JOLLA	logc
2	1999-01-15 11:06:47.000	5	nt	610	passed	Kim	CARLSBAD	poli
3	1999-01-15 11:05:18.000	5	nt	612	passed	Alice	LA_JOLLA	poli
4	1999-01-15 11:04:41.000	4	nt	643	passed	Tom	TORREY_PINES	acco
5	1999-01-15 11:04:39.000	4	nt	643	passed	Dave	VISTA	acco
6	1999-01-15 11:04:19.000	4	nt	643	passed	Dave	VISTA	acco
7	1999-01-15 11:02:55.000	4	nt	608	passed	Tom	TORREY_PINES	poli
8	1999-01-15 11:01:32.000	4	nt	808	passed	Dave	VISTA	poli
9	1999-01-15 11:00:24.000	4	nt	808	passed	Tom	TORREY_PINES	poli
10	1999-01-15 11:00:08.000	3	nt	625	passed	Mike	SANTA_FE	acco
11	1999-01-15 10:59:40.000	3	nt	625	passed	Kim	CARLSBAD	acco
12	1999-01-15 10:59:03.000	3	nt	625	passed	Dave	VISTA	acco
13	1999-01-15 10:58:29.000	3	nt	535	passed	Dave	VISTA	logc
14	1999-01-15 10:57:15.000	3	nt	535	passed	Alice	LA_JOLLA	logc
15	1999-01-15 10:57:12.000	3	nt	535	passed	Kim	CARLSBAD	logc
16	1999-01-15 10:55:26.000	3	nt	2	passed	Cindy	ENCINITAS	unk
17	1999-01-15 10:52:16.000	2	nt	640	passed	Dave	VISTA	acco
18	1999-01-15 10:49:33.000	2	nt	513	passed	Kim	CARLSBAD	syst
19	1999-01-15 10:47:45.000	2	nt	634	passed	Alice	LA_JOLLA	acco
20	1999-01-15 10:43:11.000	2	nt	512	passed	Tom	TORREY_PINES	syst
21	1999-01-15 10:42:08.000	2	nt	633	passed	Cindy	ENCINITAS	acco
22	1999-01-15 10:35:47.000	1	nt	560	passed	Steve	CARDIFF	obje
23	1999-01-15 10:31:48.000	5	cmds	10021	passed	Steve	CARDIFF	aler
24	1999-01-15 10:31:48.000	1	nt	517	passed	Steve	CARDIFF	syst
25	1999-01-15 10:28:46.000	5	cmds	10021	passed	Dave	VISTA	aler
26	1999-01-15 10:28:46.000	1	nt	517	passed	Dave	VISTA	syst
27	1999-01-15 10:25:15.000	5	cmds	10021	passed	Alice	LA_JOLLA	aler
28	1999-01-15 10:25:15.000	1	nt	517	passed	Alice	LA_JOLLA	syst
29	1999-01-15 10:24:52.000	1	nt	560	passed	Mike	SANTE_FE	obje
30	1999-01-15 10:22:24.000	0	nt	504	passed	Dave	VISTA	dat

Data Profiles Charts

There are 33 records in the result set. 33 record(s) loaded.

DateLine: Tuesday, 11:02 AM, West Coast Product&Sales Building

**Filter Audit Data** **Filter Audit Data** **Filter Audit Data** ✕

Select Events Interval: **Events Interval:** Custom ▾

Start Time/Date: Start Time: 09:45:00 End Time/Date: End Time: 11:45:00  
 Start Date: 01/15/1999 End Date: 01/15/1999

Select Filters: **Filters:**

Computer Name	Event Category	Event Source Log	Resolution
Severity	Operating System	Event Number	Event Type
Severity	Operating System	Event Number	Event Type

Choices: 0 1 2 3 4 5

Choices: 0 1 2 3

Choices: 0 1 2 3

Selections: 4 5

OK Cancel OK Cancel Apply Reset Details...

Filtering on the highest severity events, security can quickly determine potential misuse...

DateLine: Tuesday, 11:03 AM, West Coast Product&Sales Building





Computer Misuse Detection System

Log Data Help



Unacknowledged Event Status

- 5 Network
  - 5 My Domain
    - 5 My Workgroup
      - 5 CARDIFF
      - 5 CARLSBAD
      - 0 DEL\_MAR
      - 3 ENCINITAS
      - 5 LA\_JOLLA
      - 3 SANTA\_FE
      - 1 SANTE\_FE
      - 4 TORREY\_PINES
      - 5 VISTA

Event Details - Row 10

Time Generated: 1999-01-15 10:31:48.000

User Name: Steve

Severity: 5

Computer Name: CARDIFF

Operating System: cmds

Event Category: alert

Event Number: 10021

Event Source Log: analyzer

Event Type: passed

Resolution: 3

Event Analysis

The audit log was cleared!

Close

Previous

Next

Data Profiles Charts

There are 12 records in the result set. 12 record(s) loaded.



Security is alerted on unusual traffic patterns as well as single actions, like a hacker covering his tracks...

DateLine: Tuesday, 11:04 AM, West Coast Product&Sales Building

Computer Misuse Detection System

Log Data Help

Unacknowledged Event Status

Unacknowledged

- 5 Network
  - 5 My Domain
    - 5 My Work
      - 5 CARL
      - 0 DEL
      - 3 ENC
      - 5 LA\_J
      - 3 SANT
      - 1 SANT
      - 4 TORR
      - 5 VISTA
    - 3 My Do
      - 1
      - 3
      - 0
      - 3
      - 0
      - 3
      - 2
      - 3
  - 0 Network
    - 0 My Workgroup
      - 0 CARDIFF
      - 0 CARLSBAD
      - 0 DEL\_MAR
      - 0 ENCINITAS
      - 0 LA\_JOLLA
      - 0 SANTA\_FE
      - 0 SANTE\_FE
      - 0 TORREY\_PINES
      - 0 VISTA

Event Log

	Time	Severity	Operating System	Event Number	Event Type	User Name	Computer Name	Ev
1	1999-01-15 11:06:58.000	5	nt	534	passed	Alice	LA_JOLLA	logd
						Kim	CARLSBAD	poll
						Alice	LA_JOLLA	poll
						Tom	TORREY_PINES	acce
						Dave	VISTA	acce
						Dave	VISTA	acce
						Tom	TORREY_PINES	poll
						Dave	VISTA	poll
						Tom	TORREY_PINES	poll
						Mike	SANTA_FE	acce
						Kim	CARLSBAD	acce
						Dave	VISTA	acce
						Dave	VISTA	logd
						Alice	LA_JOLLA	logd
						Kim	CARLSBAD	logd
						Cindy	ENCINITAS	unkr
						Dave	VISTA	acce
						Kim	CARLSBAD	syst
						Alice	LA_JOLLA	acce
						Tom	TORREY_PINES	syst
						Cindy	ENCINITAS	acce
						Steve	CARDIFF	obje
						Steve	CARDIFF	aler
						Steve	CARDIFF	syst
25	1999-01-15 10:28:46.000	5	cmds	10021	passed	Dave	VISTA	aler
26	1999-01-15 10:28:46.000	1	nt	517	passed	Dave	VISTA	syst
27	1999-01-15 10:25:15.000	5	cmds	10021	passed	Alice	LA_JOLLA	aler
28	1999-01-15 10:25:15.000	1	nt	517	passed	Alice	LA_JOLLA	syst
29	1999-01-15 10:24:52.000	1	nt	560	passed	Mike	SANTA_FE	obje
30	1999-01-15 10:22:34.000	0	nt	594	passed	Dave	VISTA	det

Then security acknowledges those events...

OK Apply Cancel

There are 33 records in the result set. 33 record(s) loaded.

Done, acknowledging viewable records.

There are 12 records in the result set. 12 record(s) loaded.

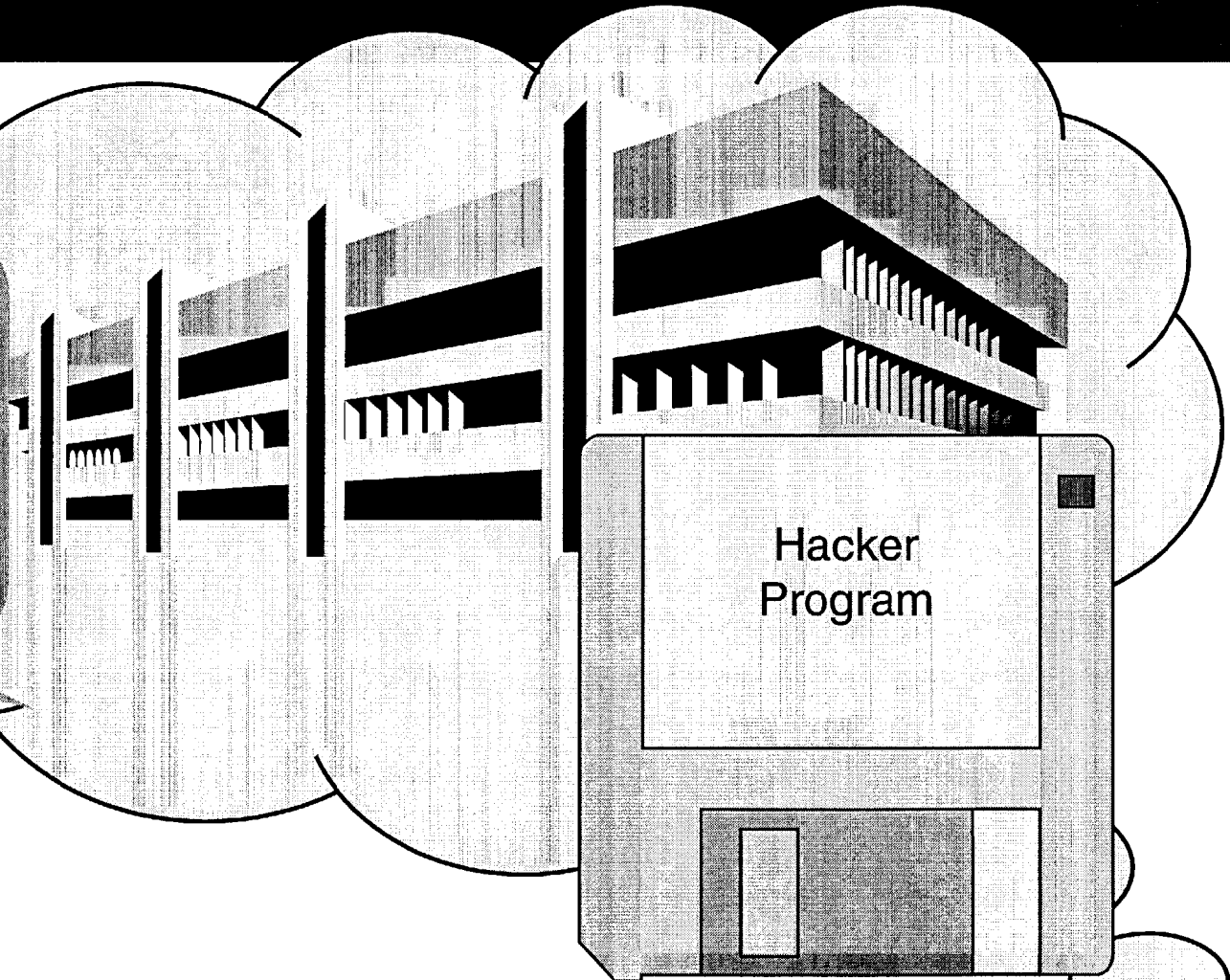
DateLine: Tuesday, 11:09 AM, West Coast Product&Sales Building

Later that day,  
Alice, a mid-level  
manager, leaves  
for lunch, but  
forgets to lock her  
workstation...



**DateLine: Tuesday, 11:45 AM, West Coast Product&Sales Building**

Shortly after leaving her office, Kurt enters Alice's office with a utility that will give him root access to Alice's machine...



**DateLine: Tuesday, 11:57 AM, West Coast Product&Sales Building**



Computer Misuse Detection System

Log Data Help



### Unacknowledged Event Status

- 5 Network
  - 5 West Coast
    - 5 Product&Sales
      - 1 CARDIFF
      - 4 CARLSBAD
      - 0 DEL\_MAR
      - 3 ENCINITAS
      - 5 LA\_JOLLA
      - 3 SANTA\_FE
      - 1 SANTE\_FE
      - 4 TORREY\_PINES
      - 4 VISTA

At the security center, CMDS alerts on suspicious events for Alice's computer...

### Event Log

	Time	Severity	Operating System	Event Number	Event Type	User Name	Computer Name	Ev
41	1999-01-15 11:51:31.000	1	nt	560	passed	Kim	CARLSBAD	obje
42	1999-01-15 11:51:52.000	1	nt	560	passed	Mike	SANTE_FE	obje
43	1999-01-15 11:52:15.000	1	nt	560	passed	Alice	LA_JOLLA	obje
44	1999-01-15 11:52:46.000	1	nt	560	passed	Dave	VISTA	obje
45	1999-01-15 11:52:48.000	1	nt	560	passed	Steve	CARDIFF	obje
46	1999-01-15 11:53:17.000	1	nt	560	passed	Steve	CARDIFF	obje
47	1999-01-15 11:53:48.000	2	nt	633	passed	Cindy	ENCINITAS	acce
48	1999-01-15 11:54:11.000	2	nt	512	passed	Tom	TORREY_PINES	syst
49	1999-01-15 11:54:15.000	2	nt	634	passed	Alice	LA_JOLLA	acce
50	1999-01-15 11:54:33.000	2	nt	513	passed	Kim	CARLSBAD	syst
51	1999-01-15 11:54:36.000	2	nt	640	passed	Dave	VISTA	acce
2	1999-01-15 11:55:16.000	3	nt	2	passed	Cindy	ENCINITAS	unke
3	1999-01-15 11:55:22.000	3	nt	535	passed	Kim	CARLSBAD	logc
4	1999-01-15 11:55:25.000	5	cmds	10020	passed	Alice	LA_JOLLA	aler
5	1999-01-15 11:55:25.000	2	nt	592	passed	Alice	LA_JOLLA	deta
6	1999-01-15 11:55:31.000	4	cmds	10016	passed	Alice	LA_JOLLA	want
7	1999-01-15 11:55:31.000	2	nt	632	passed	Alice	LA_JOLLA	acce
8	1999-01-15 11:56:29.000	3	nt	535	passed	Dave	VISTA	logc
9	1999-01-15 11:57:14.000	3	nt	625	passed	Kim	CARLSBAD	acce
0	1999-01-15 11:57:31.000	3	nt	625	passed	Dave	VISTA	acce
1	1999-01-15 11:57:38.000	3	nt	625	passed	Mike	SANTA_FE	acce
62	1999-01-15 11:57:44.000	4	nt	608	passed	Tom	TORREY_PINES	poli
63	1999-01-15 11:57:52.000	4	nt	608	passed	Dave	VISTA	poli
64	1999-01-15 11:58:15.000	4	nt	608	passed	Tom	TORREY_PINES	poli
65	1999-01-15 11:58:19.000	4	nt	643	passed	Dave	VISTA	acce
66	1999-01-15 11:58:39.000	4	nt	643	passed	Dave	VISTA	acce
67	1999-01-15 11:59:41.000	4	nt	643	passed	Tom	TORREY_PINES	acce
68	1999-01-15 11:59:48.000	4	nt	643	passed	Alice	LA_JOLLA	acce
69	1999-01-15 11:59:57.000	4	nt	608	passed	Kim	CARLSBAD	poli
70	1999-01-15 11:59:58.000	4	nt	643	passed	Alice	LA_JOLLA	acce

Data Profiles Charts

Sorting: Column Completed.



DateLine: Tuesday, 12:02 PM, West Coast Product&Sales Building



## Event Details - Row 54

Time Generated: 1999-01-15 11:5  
Severity: 5  
Operating System: cmds  
Event Number: 10020  
Event Type: passed

## Event Analysis

CMDS has detected the sechole ex

Security is able to quickly determine that a hacker program was executed...

## Event Details - Row 56

Time Generated: 1999-01-15 11:55:31.000 User Name: Alice  
Severity: 4 Computer Name: LA\_JOLLA  
Operating System: cmds Event Category: warning  
Event Number: 10016 Event Source Log: analyzer  
Event Type: passed Resolution: 3

## Event Analysis

CMDS has detected a change to the Administrators, Domain Administrators, or Power Users groups.

And that a change to Admin has occurred...

Close

Previous

Next

At the end of the day Alice leaves for home, only to have Kurt enter her office and begin downloading sensitive data...



**DateLine: Tuesday, 5:34 PM, West Coast Product&Sales Building**



Computer Misuse Detection System

Log Data Help



### Unacknowledged Event Status

- 5 Network
  - 5 West Coast
    - 5 Product&Sales
      - 1 CARDIFF
      - 3 CARLSBAD
      - 0 DEL\_MAR
      - 3 ENCINITAS
      - 5 LA\_JOLLA
      - 3 SANTA\_FE
      - 1 SANTE\_FE
      - 4 TORREY\_PINES
      - 4 VISTA

In the security center, CMDS alerts the security officer to suspicious activity on Alice's computer...

### Event Log

	Time Generated	Severity	Operating System	Event Number	Event Type	User Name	Computer Name	Ev
2	1999-01-15 05:50:11.000	0	nt	593	passed	Nicole	DEL_MAR	deta
3	1999-01-15 05:50:18.000	0	nt	562	passed	Steve	CARDIFF	obje
4	1999-01-15 05:50:21.000	0	nt	593	passed	Nicole	DEL_MAR	deta
5	1999-01-15 05:51:14.000	0	nt	594	passed	Dave	VISTA	deta
6	1999-01-15 05:51:21.000	1	nt	560	passed	Kim	CARLSBAD	obje
7	1999-01-15 05:51:24.000	0	nt	594	passed	Dave	VISTA	deta
8	1999-01-15 05:51:31.000	1	nt	560	passed	Kim	CARLSBAD	obje
9	1999-01-15 05:51:52.000	1	nt	560	passed	Mike	SANTE_FE	obje
10	1999-01-15 05:52:15.000	1	nt	560	passed	Alice	LA_JOLLA	obje
11	1999-01-15 05:52:46.000	1	nt	560	passed	Dave	VISTA	obje
12	1999-01-15 05:52:48.000	1	nt	560	passed	Steve	CARDIFF	obje
13	1999-01-15 05:53:17.000	1	nt	560	passed	Steve	CARDIFF	obje
14	1999-01-15 05:53:48.000	2	nt	633	passed	Cindy	ENCINITAS	acco
15	1999-01-15 05:54:11.000	2	nt	512	passed	Tom	TORREY_PINES	syst
16	1999-01-15 05:54:15.000	2	nt	634	passed	Alice	LA_JOLLA	acco
17	1999-01-15 05:54:33.000	2	nt	513	passed	Kim	CARLSBAD	syst
18	1999-01-15 05:54:36.000	2	nt	640	passed	Dave	VISTA	acco
19	1999-01-15 05:55:16.000	3	nt	2	passed	Cindy	ENCINITAS	unk
20	1999-01-15 05:55:17.000	1	nt	560	passed	Guest	LA_JOLLA	obje
21	1999-01-15 05:55:22.000	3	nt	535	passed	Kim	CARLSBAD	logc
22	1999-01-15 05:55:25.000	5	cmds	10006	passed	Guest	LA_JOLLA	aler
23	1999-01-15 05:55:25.000	2	nt	528	passed	Guest	LA_JOLLA	logc
24	1999-01-15 05:55:31.000	1	nt	560	passed	Guest	LA_JOLLA	obje
25	1999-01-15 05:56:29.000	3	nt	535	passed	Dave	VISTA	logc
26	1999-01-15 05:57:14.000	3	nt	625	passed	Kim	CARLSBAD	acco
27	1999-01-15 05:57:19.000	1	nt	560	passed	Guest	LA_JOLLA	obje
28	1999-01-15 05:57:21.000	1	nt	560	passed	Guest	LA_JOLLA	obje
29	1999-01-15 05:57:30.000	1	nt	560	passed	Guest	LA_JOLLA	obje
30	1999-01-15 05:57:31.000	3	nt	625	passed	Dave	VISTA	acco
31	1999-01-15 05:57:39.000	2	nt	625	passed	Mike	SANTA_FE	acco

Data Profiles Charts

Sorting: Column Completed

DateLine: Tuesday, 5:38 PM, West Coast Product&Sales Building



Event Details - Row 22

Time Generated:	1999-01-15 05:55:25.000	User Name:	Guest
Severity:	5	Computer Name:	LA_JOLLA
Operating System:	cmds	Event Category:	alert
Event Number:	10006	Event Source Log:	analyzer
Event Type:	passed	Resolution:	3

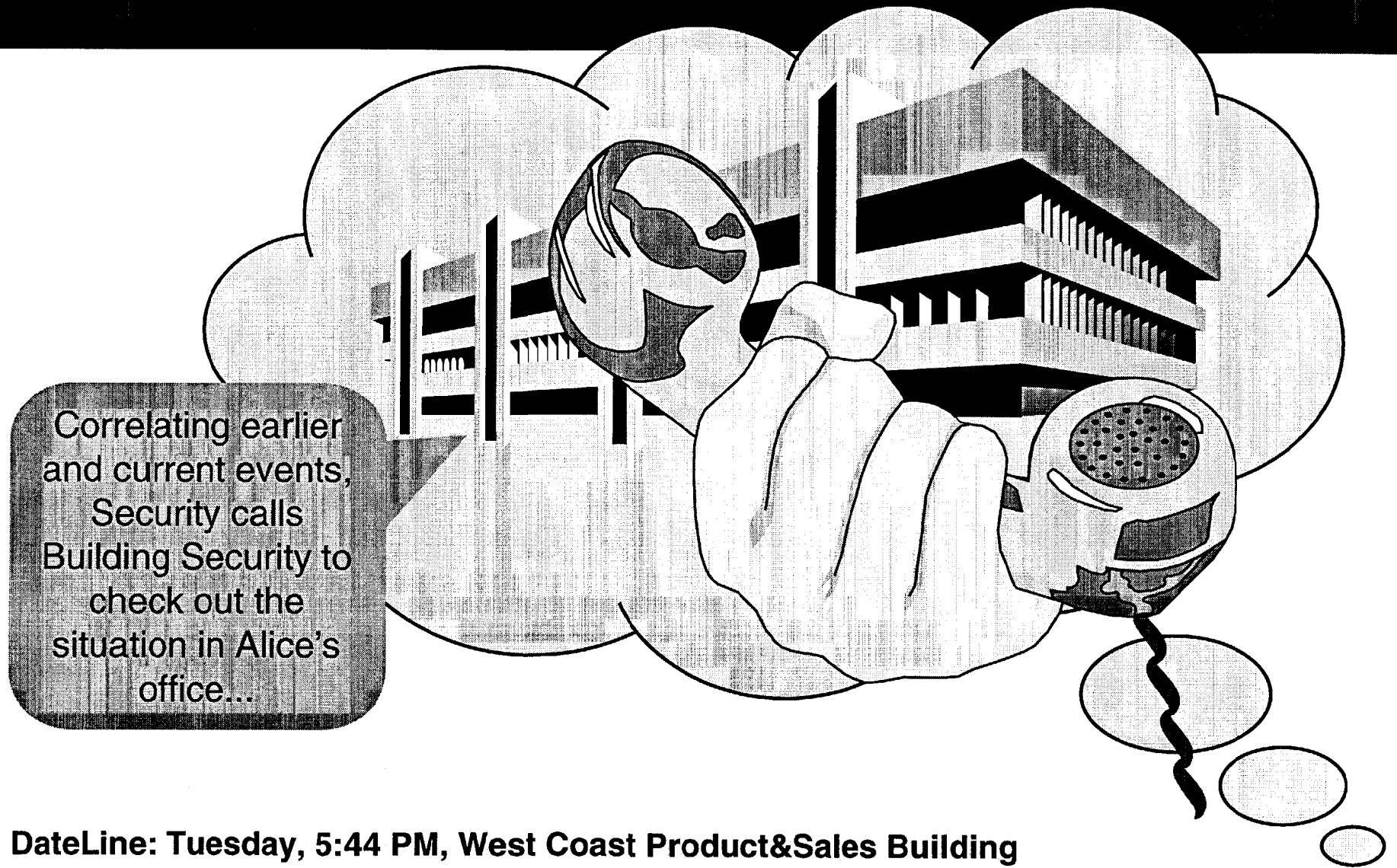
Event Analysis

A non-interactive service account was logged into!

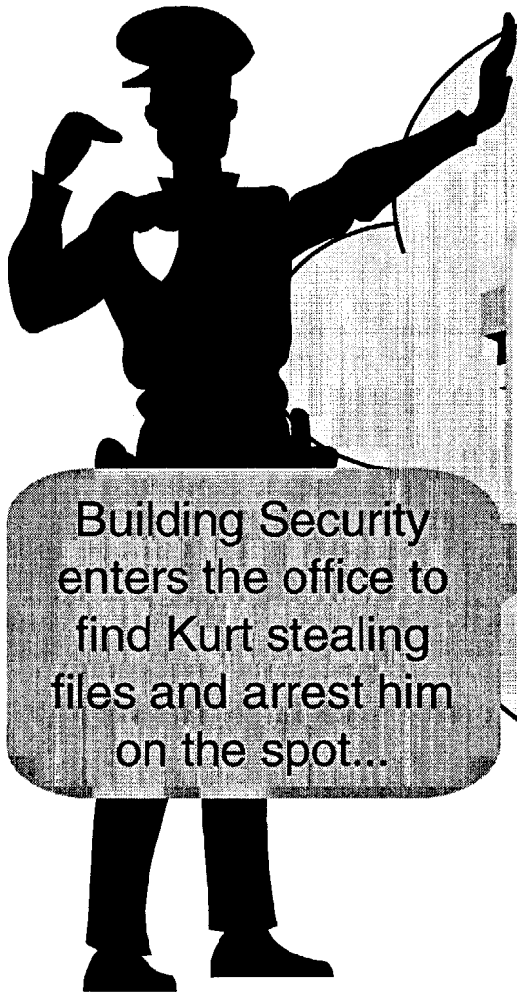
Close Previous Next

Security obtains further details that an Unauthorized User has logged on Alice's computer...

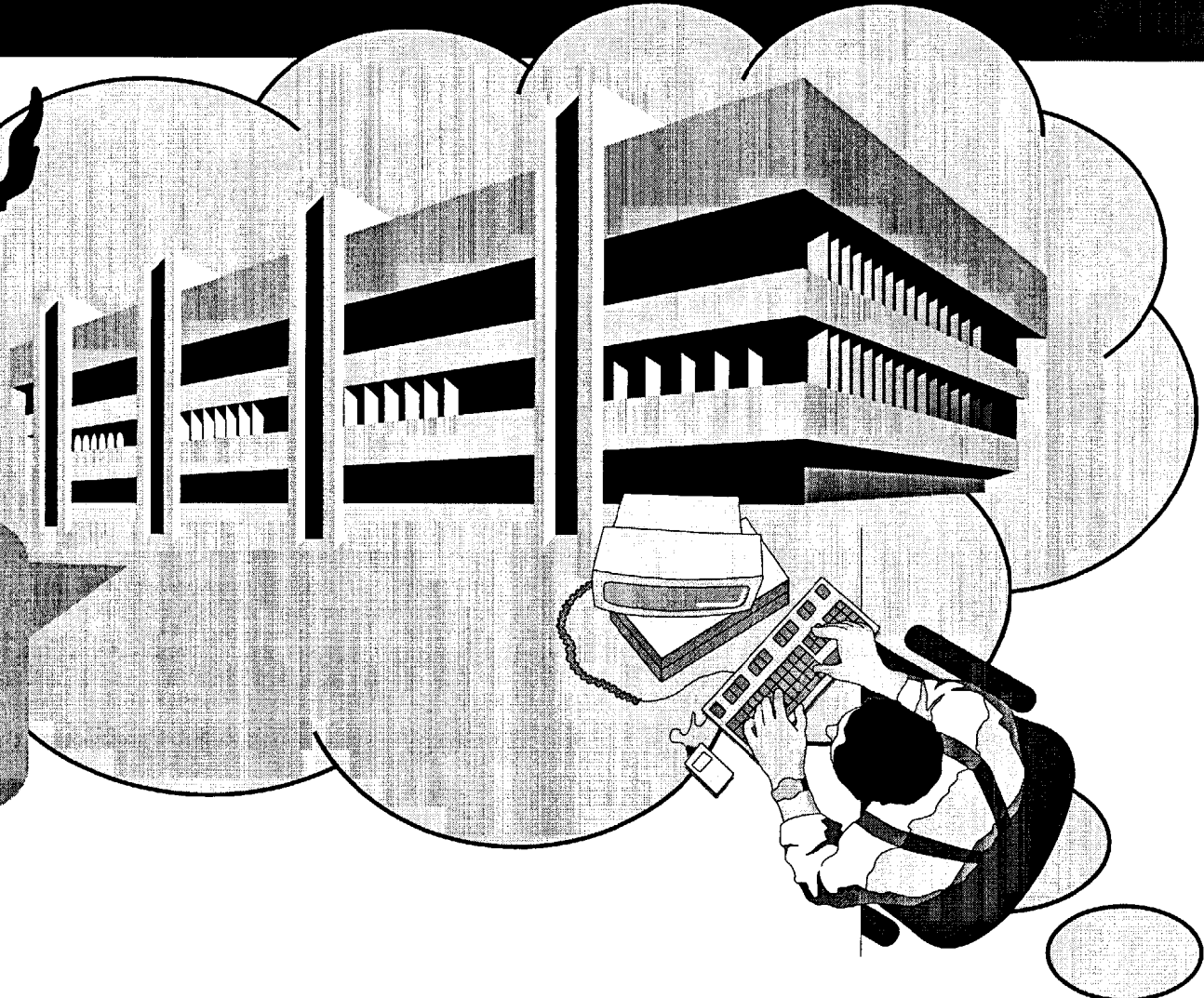
DateLine: Tuesday, 5:39 PM, West Coast Product&Sales Building



**DateLine: Tuesday, 5:44 PM, West Coast Product&Sales Building**



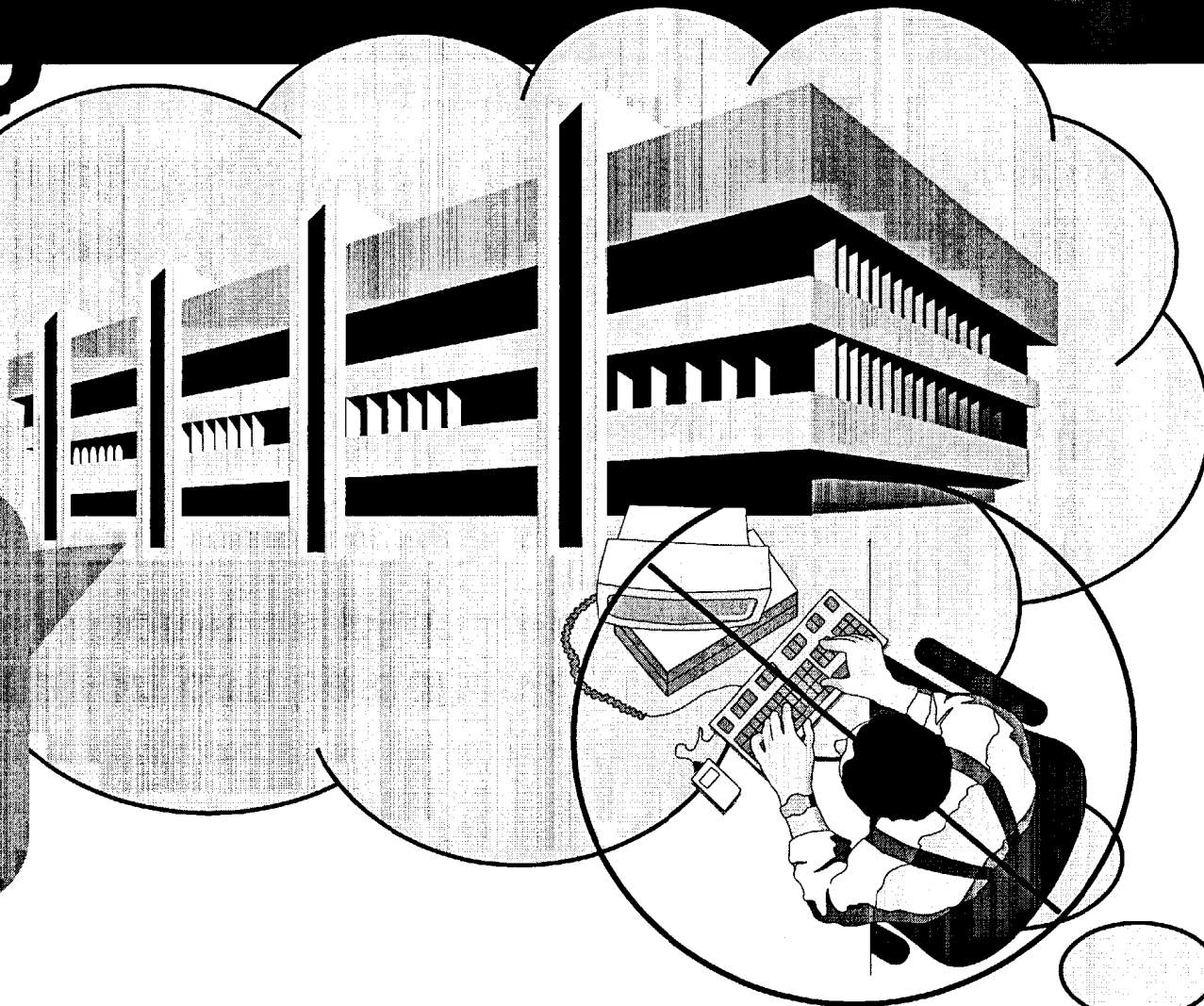
Building Security  
enters the office to  
find Kurt stealing  
files and arrest him  
on the spot...



**DateLine: Tuesday, 5:49 PM, West Coast Product&Sales Building**



Building Security  
contacts proper  
authorities about  
the arrest. A CMDS  
report is prepared  
of the event trail for  
prosecution...



**DateLine: Tuesday, 5:56 PM, West Coast Product&Sales Building**



## ***Benefits of CMDStm Enterprise***

- **Event information can be collected from disparate systems into a common platform**
- **Event data can be managed at its location or centrally**
- **Detection and monitoring of unauthorized access by employees, including system administration personnel**



## ***Benefits of CMDStm Enterprise (cont'd)***

- **Security policy monitoring on a 7X24 basis**
- **Profiles of user(s) dynamically created to identify account hi-jacking, - Last Line of Defense**
- **Archival & Retrieval of Raw Audit Data aids in the Contingency Planning Process**



## ***ODS Summary Topics***

- **Air Force and NATO deployments of SecureCom**
- **Integration of routers, firewalls, VPN, IDS, hosts, and a conversation aware infrastructure within the CMDS expert system.**
- **Questions on SecureCom and CMDS:**
  - **Scaling Up to necessary Speeds, the McKinley engine project.**
- **Questions.**



# ***SecureCom Security Platform, Alias: DMZ in a box, LAN in a can...***

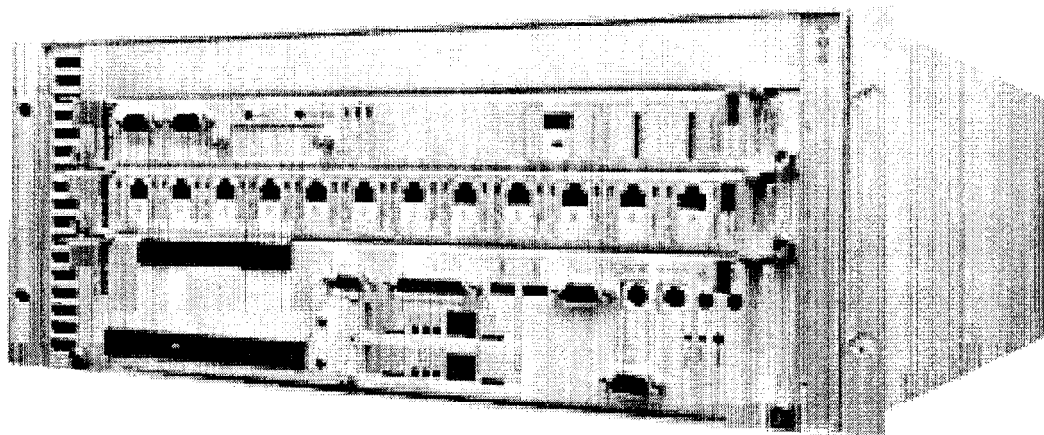
**Network Connectivity**

**Pentium PC/Sun / HP Modules**

**ODS Security Software**

**Third Party Software, multi-port probe firmware.**

**Easy To  
Install  
and  
Manage**



**Lean,  
Light, &  
Lethal**

**Infrastructure  
and  
Traffic  
Monitoring**  
  
**(ProtoCop)**

**Network  
& Host  
Based IDS**  
**(RealSecure)**  
**(NetRanger)**  
**(CMDS)**  
**(NFR)**

**Authentication  
& Encryption  
VPN**  
  
**(Crypto  
Watch)**

**Firewalls**  
  
**(Raptor)**  
**(Firewall 1)**  
**(Lucent)**  
**(Gauntlet)**  
**(PIX)**

**NT,  
Sun,  
HP Servers**  
  
**(Flexible)**

**Multivendor  
Profiling  
&  
Correlation**  
  
**(CMDS  
Enterprise)**

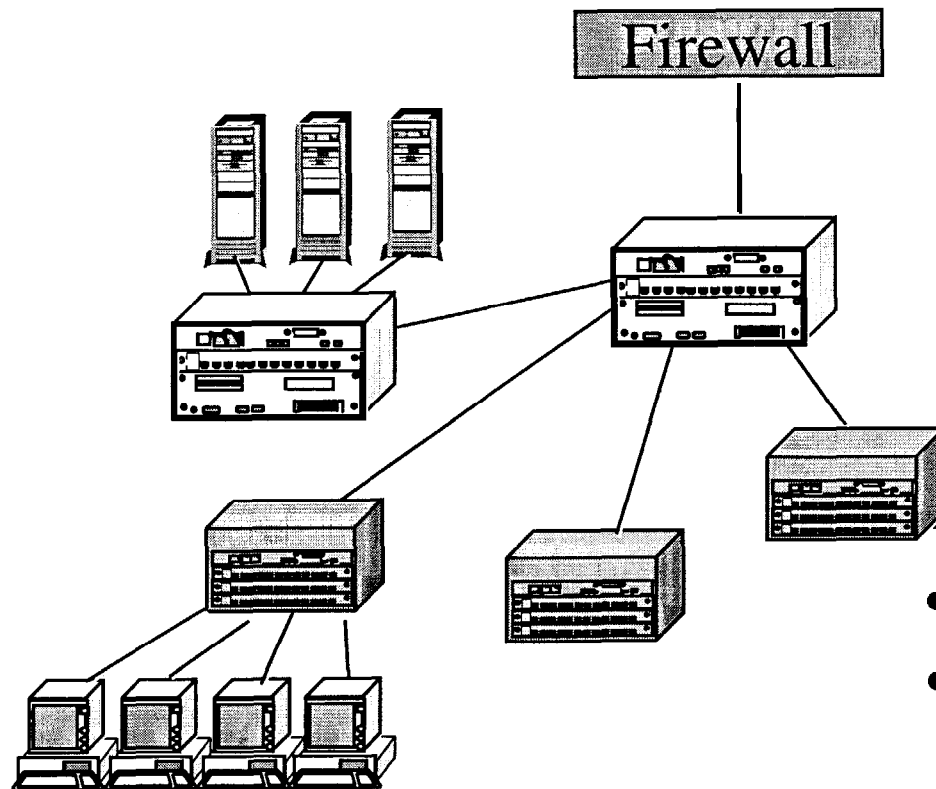




## ***Current Speed Limits of Security***

- Security management requires Layers 3, 4, and above
- Speed Limits of prior technology - Existing IDS and Firewall Limits
  - ASICs and processor combinations limited to less than 100 Mb/s
- How to manage and secure at Gigabit and Terabit LAN speeds?
  - Can't drink from a fire hose without specialized hardware
  - Analysis at 1 Gb/s and above
  - ODS String Search Engine as a firewall, IDS, profiler on steroids

# Typical Challenges in Today's Environment



- **Server & Users**

- Fast Ethernet
- OC3 / OC12
- Gig Ethernet or Fiber Channel
- Hippi 800
- GSN / 10 Gig Ethernet

Over-subscription: where?

- Trunking
- Where billing and security?



## ***ODS String Search Engine***

- **Hardware Joshua Tree**
- **3 Year Development**
- **Full 7 Layer Decoding**
- **First Prototype: 2.2 Mpps with 1 Million Strings**
- **Production ASIC: 12 Mpps with 1+ Million Strings**
- **Pattern matching scalable to fit any requirement**



## ***Applications of String Search Engine***

- 1 Gb/s conversation analysis for OC3/12, GE, Hippi 800
- OC12 and GE Encryption box
- GSN or 10 Gigabit Probe
- Hardware CERT Attack Filter
- Custom Probes for specialized data selection and collection
- Gigabit Firewall that also provides full IDS, billing, and upper layer decodes to feed user profile analysis for habit monitoring by CMDS.



## *High Speed Packet Engine (HSPE)*

- **Hardware Components**

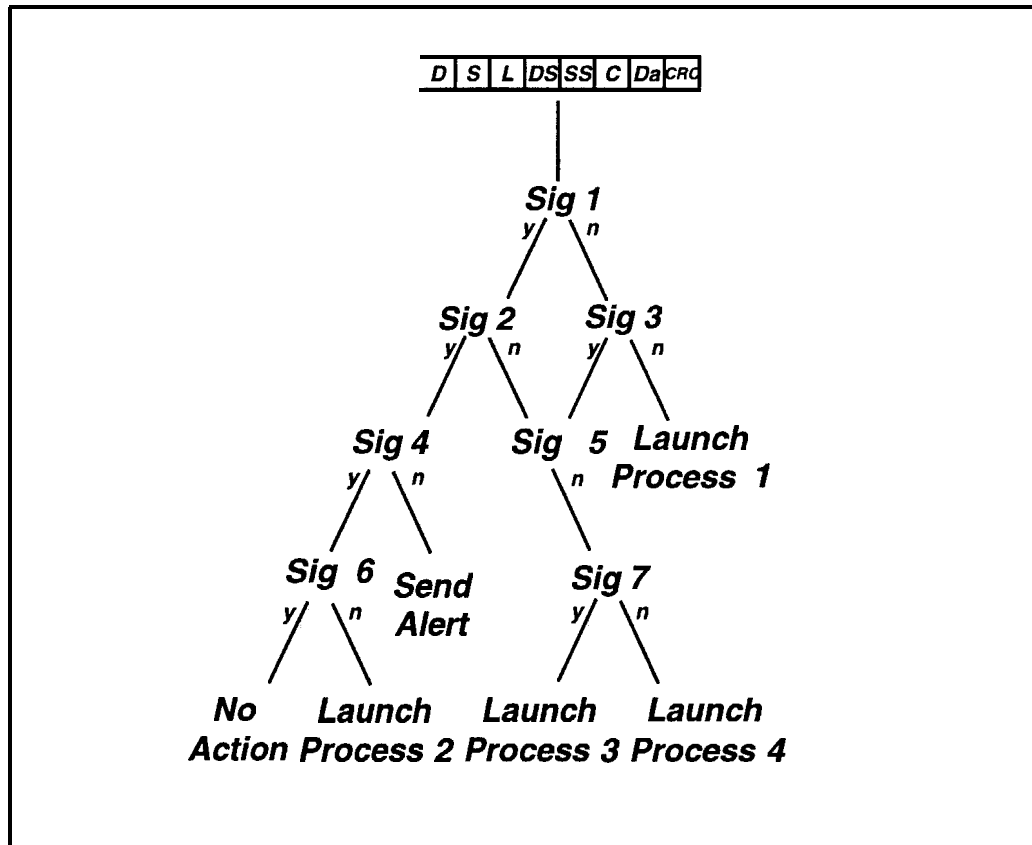
- Hardware Interface, memory, packet engine, & CPU
- Hardware can be integrated to other processes
  - RMON, Firewall, Encryption, Authentication, Routing, Switching

- **Simple Program Language**

- Tells engine where to look in packet; bit(s)/bytes or range
- Recognizes patterns found in packet and matches to programmed signatures
  - Conversation pairs, packet data, protocol analysis, data descriptions

- **Provides Descriptors**

- Allows commands to be sent when matches found
- Match handle is a 24 bit number
- Internal counters can accumulate statistics of each match



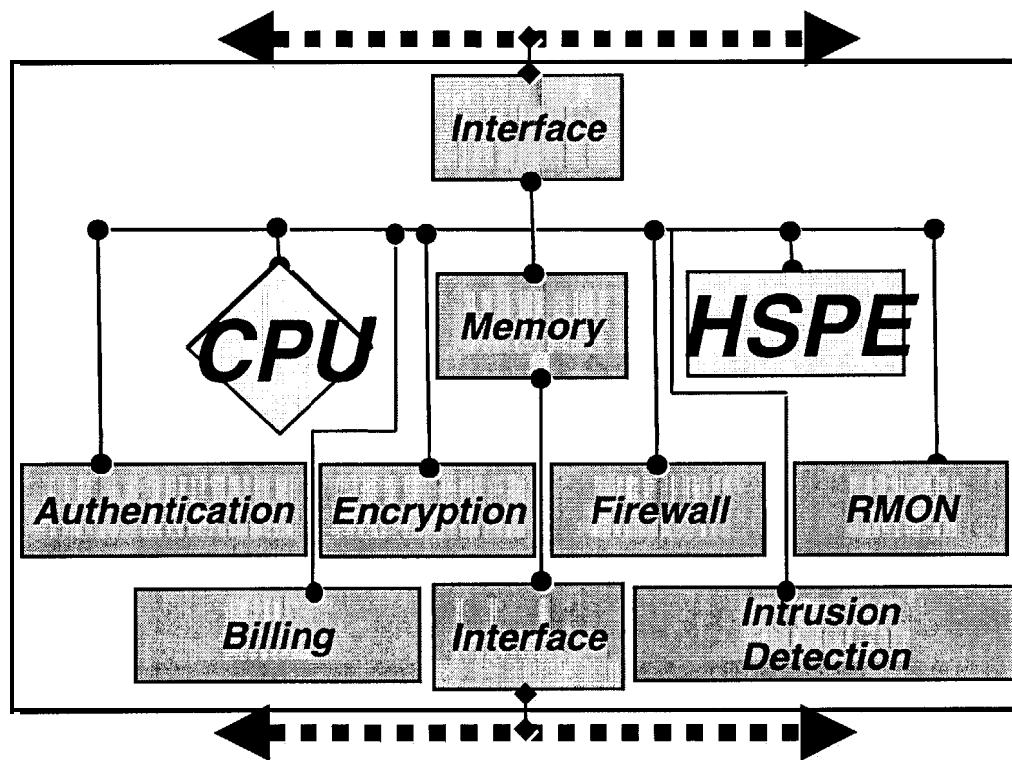
## • Pattern Recognition

- Simple single patterns  
bit or byte
- Complex patterns or  
ranges
- Nested patterns

## • Pattern Response

- Send descriptor to
  - Log
  - Alert
  - Launch process
- Look for next pattern

- **High Speed Packet Filtering**
  - Packet filtering rate of 700,000 to 5 million packets per second
- **Numerous Signatures can be Programmed**
  - From 100,000 to 1 million signatures
  - Simple, complex or nested signatures
- **Looks Anywhere in the Packet**
  - Can be programmed to look for bit/byte patterns in packet header, payload, or, over multiple packets







## ***HSPE Advantages***

- **Provides Wire-Speed Filtering**
  - Reviews packets at over Gigabit speeds
  - Finds matches in packets with pre-defined signatures
  - When matches found sends “commands” to other processes based on pre-set filter criteria
- **Can be Attached in Numerous Ways**
  - As a faster Firewall, IDS, or user profiler
  - In between “Up-links” between switches or routers
  - At connection points LAN to LAN, LAN to WAN, WAN to WAN
- **Only hope above 100 Mb/s. Runs currently at 2 Gb/s, scales to 10 Gb/s links.**



## ***Contact Information***

- **Dave Steinman      - DC**
  - DC Special Programs Manager
  - [dsteinman@ods.com](mailto:dsteinman@ods.com)
  - 7031506-1 167
- **Mike Celiceo      - San Diego**
  - CMDS Product Specialist
  - [mceliceo@ods.com](mailto:mceliceo@ods.com)
  - (619) 2684236 ext. 2232
- **Joe Head      - Dallas**
  - Executive VP
  - [head@ods.com](mailto:head@ods.com)
  - 972/301-3636